Evoluzione di OSINT e operazioni militari che non sono più segrete

Maria Cattini | 22/02/2025 | Open source intelligence

Negli ultimi dieci anni, il mondo dell'**Open Source Intelligence (OSINT)** e dell'**Imagery Intelligence (IMINT)** ha subito una trasformazione radicale. Nell'era digitale, il concetto di "operazione segreta" sta rapidamente perdendo significato. L'Open Source Intelligence (OSINT) ha trasformato radicalmente il panorama dell'intelligence militare, rendendo sempre più difficile mantenere la riservatezza delle operazioni. Questi strumenti, un tempo appannaggio esclusivo delle agenzie governative, sono diventati accessibili al pubblico, rivoluzionando il modo in cui raccogliamo e analizziamo le informazioni.

Nel 2014, durante l'annessione della Crimea da parte della Russia, le immagini satellitari disponibili al pubblico erano scarse e di bassa risoluzione. Le informazioni provenivano principalmente da fonti ufficiali come il Dipartimento di Stato degli Stati Uniti e la NATO. Le immagini non satellitari erano limitate, anche se alcuni soldati russi si rivelarono involontariamente attraverso selfie geolocalizzati.

Oggi, la situazione è completamente diversa. La diffusione di smartphone ha raggiunto livelli senza precedenti, con circa 6,6 miliardi di dispositivi in uso, rappresentando l'84% della popolazione mondiale. Questa massiccia presenza di dispositivi mobili ha trasformato ogni individuo in un potenziale raccoglitore di informazioni. Piattaforme come TikTok e YouTube sono diventate fonti inesauribili di dati, permettendo l'identificazione di unità militari attraverso video condivisi da comuni cittadini.

Trasformazioni chiave introdotte dall'OSINT

• Accesso democratizzato all'informazione:Chiunque, da giornalisti a attivisti, può accedere a dati satellitari (es. Maxar, Planet Labs), social media (Twitter, Telegram), forum pubblici, e database governativi aperti. Strumenti come Google Earth o Flightradar24 rivelano movimenti di truppe o aerei militari in tempo quasi reale. Tra le novità più rilevanti, Google ha reso disponibili immagini open source ad alta risoluzione, datate 24 novembre 2023, tramite le piattaforme Google Earth e Google Earth Pro, le prime gratuite disponibili dopo il 7 ottobre.
• Analisi in tempo reale e crowdsourcing:Piattaforme come Bellingcat utilizzano OSINT per indagare su crimini di guerra (es. attacchi chimici in Siria) o tracciare movimenti militari (es. concentrazioni di carri armati ai confini ucraini nel 2022). Anche cittadini comuni contribuiscono condividendo foto/video su TikTok o Telegram.
• Verifica incrociata delle fonti:L’intelligence tradizionale viene contestata se contraddetta da prove OSINT. Esempio: le immagini satellitari di Maxar hanno smascherato dinieghi su operazioni militari in Yemen o Myanmar.
• Sfruttamento di metadati:Foto o video condivisi online contengono dati EXIF (geolocalizzazione, ora), utili per ricostruire eventi. Nel 2020, i metadati di un video hanno confermato la posizione di soldati turchi in Libia.

Sfide alla riservatezza militare

• Fughe involontarie da social media:Militari o contractor che postano selfie, anche cancellati, lasciano tracce. Nel 2021, un video TikTok ha rivelato la posizione di un sottomarino nucleare statunitense.

• Satelliti commerciali ad alta risoluzione:Aziende come Capella Space (satelliti radar) o BlackSky forniscono immagini notte/giorno, utilizzate per monitorare basi militari o movimenti di droni.
• Analisi algoritmica e AI:Strumenti di machine learning (es. Palantir) processano grandi volumi di dati OSINT per identificare pattern, come l'attivazione di sistemi di difesa aerea.
• Crowdsourcing di avversari:Gruppi come i hacker russi o Anonymous raccolgono OSINT per colpire infrastrutture critiche nemiche, sfruttando dati pubblici su reti elettriche o comunicazioni.

Esempi concreti di impatto OSINT

• Ucraina (2022-in corso):OSINT ha documentato atrocità (es. massacro di Bucha) e tracciato distruzioni via satelliti. Anche i civili hanno mappato colonne russe su Google Maps.
• Assassinio di Qasem Soleimani (2020):Analisti hanno ricostruito l'attacco tramite dati ADS-B (tracciamento aereo) e foto dei rottami del drone statunitense.
• Guerra in Siria:Organizzazioni come Syrian Archive hanno usato OSINT per identificare responsabili di attacchi a ospedali, incrociando video locali e dati geospaziali. Un'inchiesta realizzata attraverso immagini satellitari è stata pubblicata da BBC Verify il 23 gennaio. Grazie alle immagini fornite da Planet Lab, l'emittente britannica è riuscita a verificare come le Forze di difesa israeliane (Idf) stiano costruendo infrastrutture all'interno della zona cuscinetto demilitarizzata che separa le Alture del Golan – occupate da Israele – dalla Siria. Secondo i termini dell'accordo di cessate il fuoco tra i due Paesi del 1974, questa zona dovrebbe rimanere interdetta. La notizia è stata ulteriormente approfondita dai giornalisti di Al Jazeera, che hanno rilevato la costruzione di sei strutture all'interno della zona cuscinetto.
Le mappe sviluppate da The Conversation analizzano gli impatti del conflitto sui terreni agricoli (a sinistra) e le serre (a destra) della striscia di Gaza fra ottobre 2023 e settembre 2024

Contromisure militari per mitigare i rischi OSINT

• OPSEC (Operational Security) rafforzata:Linee guida rigorose per personale militare: divieto di smartphone in zone operative, formazione su rischi social media, uso di VPN e crittografia.
• Deception digitale:Diffusione di informazioni false per confondere avversari. Esempio: falsi piani di invasione o immagini satellitari manipolate.
• Limitazione dei dati pubblici:Governi censurano piattaforme (es. Russia con Telegram nel 2018) o ritardano pubblicazione di immagini satellitari sensibili.
• Tecnologie anti-OSINT:Camuffamento di infrastrutture militari con reti mimetiche (contro satelliti), uso di droni "kamikaze" per distruggere dispositivi elettronici nemici che raccolgono dati.

Futuro e tendenze emergenti

• AI generativa e deepfake:Video falsi potrebbero essere usati per disinformazione, sfidando l'affidabilità dell'OSINT. Serviranno tool di verifica avanzati (es. Intel's FakeCatcher).
• Internet satellitare (Starlink):Fornisce connettività in zone di guerra, accelerando il flusso di dati OSINT ma esponendo a cyberattacchi (es. interferenze russe in Ucraina).
• Etica e regolamentazione:Dibattiti su limiti alla libertà di informazione vs. sicurezza nazionale. Proposte di leggi per regolare l'uso di dati satellitari in conflitti.

Nonostante i progressi, permangono sfide significative. La sovrabbondanza di informazioni rende difficile distinguere tra dati accurati e disinformazione. Inoltre, l'uso di tecnologie avanzate da parte di attori statali e non statali richiede un costante aggiornamento delle competenze e degli strumenti OSINT. Tuttavia, con l'integrazione di intelligenza artificiale e machine learning, l'OSINT è destinato a diventare sempre più sofisticato, offrendo analisi più precise e tempestive.
Negli ultimi dieci anni, il mondo dell'**Open Source Intelligence (OSINT)** e dell'**Imagery Intelligence (IMINT)** ha subito una trasformazione radicale. Nell'era digitale, il concetto di "operazione segreta" sta rapidamente perdendo significato. L'Open Source Intelligence (OSINT) ha trasformato radicalmente il panorama dell'intelligence militare, rendendo sempre più difficile mantenere la riservatezza delle operazioni. Questi strumenti, un tempo appannaggio esclusivo delle agenzie governative, sono diventati accessibili al pubblico, rivoluzionando il modo in cui raccogliamo e analizziamo le informazioni.

Nel 2014, durante l'annessione della Crimea da parte della Russia, le immagini satellitari disponibili al pubblico erano scarse e di bassa risoluzione. Le informazioni provenivano principalmente da fonti ufficiali come il Dipartimento di Stato degli Stati Uniti e la NATO. Le immagini non satellitari erano limitate, anche se alcuni soldati russi si rivelarono involontariamente attraverso selfie geolocalizzati.

Oggi, la situazione è completamente diversa. La diffusione di smartphone ha raggiunto livelli senza precedenti, con circa 6,6 miliardi di dispositivi in uso, rappresentando l'84% della popolazione mondiale. Questa massiccia presenza di dispositivi mobili ha trasformato ogni individuo in un potenziale raccoglitore di informazioni. Piattaforme come TikTok e YouTube sono diventate fonti inesauribili di dati, permettendo l'identificazione di unità militari attraverso video condivisi da comuni cittadini.

Trasformazioni chiave introdotte dall'OSINT

• Accesso democratizzato all'informazione:Chiunque, da giornalisti a attivisti, può accedere a dati satellitari (es. Maxar, Planet Labs), social media (Twitter, Telegram), forum pubblici, e database governativi aperti. Strumenti come Google Earth o Flightradar24 rivelano movimenti di truppe o aerei militari in tempo quasi reale. Tra le novità più rilevanti, Google ha reso disponibili immagini open source ad alta risoluzione, datate 24 novembre 2023, tramite le piattaforme Google Earth e Google Earth Pro, le prime gratuite disponibili dopo il 7 ottobre.
• Analisi in tempo reale e crowdsourcing:Piattaforme come Bellingcat utilizzano OSINT per indagare su crimini di guerra (es. attacchi chimici in Siria) o tracciare movimenti militari (es. concentrazioni di carri armati ai confini ucraini nel 2022). Anche cittadini comuni contribuiscono condividendo foto/video su TikTok o Telegram.
• Verifica incrociata delle fonti:L’intelligence tradizionale viene contestata se contraddetta da prove OSINT. Esempio: le immagini satellitari di Maxar hanno smascherato dinieghi su operazioni militari in Yemen o Myanmar.
• Sfruttamento di metadati:Foto o video condivisi online contengono dati EXIF (geolocalizzazione, ora), utili per ricostruire eventi. Nel 2020, i metadati di un video hanno confermato la posizione di soldati turchi in Libia.

Sfide alla riservatezza militare

• Fughe involontarie da social media:Militari o contractor che postano selfie, anche cancellati, lasciano tracce. Nel 2021, un video TikTok ha rivelato la posizione di un sottomarino nucleare statunitense.
• Satelliti commerciali ad alta risoluzione:Aziende come Capella Space (satelliti radar) o BlackSky forniscono immagini notte/giorno, utilizzate per monitorare basi militari o movimenti di droni.
• Analisi algoritmica e AI:Strumenti di machine learning (es. Palantir) processano grandi volumi di dati OSINT per identificare pattern, come l’attivazione di sistemi di difesa aerea.
• Crowdsourcing di avversari:Gruppi come i hacker russi o Anonymous raccolgono OSINT per colpire infrastrutture critiche nemiche, sfruttando dati pubblici su reti elettriche o comunicazioni.

Esempi concreti di impatto OSINT

• Ucraina (2022-in corso):OSINT ha documentato atrocità (es. massacro di Bucha) e tracciato distruzioni via satelliti. Anche i civili hanno mappato colonne russe su Google Maps.
• Assassinio di Qasem Soleimani (2020):Analisti hanno ricostruito l’attacco tramite dati ADS-B (tracciamento aereo) e foto dei rottami del drone statunitense.
• Guerra in Siria:Organizzazioni come Syrian Archive hanno usato OSINT per identificare responsabili di attacchi a ospedali, incrociando video locali e dati geospaziali. Un'inchiesta realizzata attraverso immagini satellitari è stata pubblicata da BBC Verify il 23 gennaio. Grazie alle immagini fornite da Planet Lab, l’emittente britannica è riuscita a verificare come le Forze di difesa israeliane (Idf) stiano costruendo infrastrutture all'interno della zona cuscinetto demilitarizzata che separa le Alture del Golan – occupate da Israele – dalla Siria. Secondo i termini dell'accordo di cessate il fuoco tra i due Paesi del 1974, questa zona dovrebbe rimanere interdetta. La notizia è stata ulteriormente approfondita dai giornalisti di Al Jazeera, che hanno rilevato la costruzione di sei strutture all’interno della zona cuscinetto.
Le mappe sviluppate da The Conversation analizzano gli impatti del conflitto sui terreni agricoli (a

sinistra) e le serre (a destra) della striscia di Gaza fra ottobre 2023 e settembre 2024

Contromisure militari per mitigare i rischi OSINT

• OPSEC (Operational Security) rafforzata:Linee guida rigorose per personale militare: divieto di smartphone in zone operative, formazione su rischi social media, uso di VPN e crittografia.
• Deception digitale:Diffusione di informazioni false per confondere avversari. Esempio: falsi piani di invasione o immagini satellitari manipolate.
• Limitazione dei dati pubblici:Governi censurano piattaforme (es. Russia con Telegram nel 2018) o ritardano pubblicazione di immagini satellitari sensibili.
• Tecnologie anti-OSINT:Camuffamento di infrastrutture militari con reti mimetiche (contro satelliti), uso di droni "kamikaze" per distruggere dispositivi elettronici nemici che raccolgono dati.

Futuro e tendenze emergenti

• AI generativa e deepfake:Video falsi potrebbero essere usati per disinformazione, sfidando l'affidabilità dell'OSINT. Serviranno tool di verifica avanzati (es. Intel's FakeCatcher).
• Internet satellitare (Starlink):Fornisce connettività in zone di guerra, accelerando il flusso di dati OSINT ma esponendo a cyberattacchi (es. interferenze russe in Ucraina).
• Etica e regolamentazione:Dibattiti su limiti alla libertà di informazione vs. sicurezza nazionale. Proposte di leggi per regolare l'uso di dati satellitari in conflitti.

Nonostante i progressi, permangono sfide significative. La sovrabbondanza di informazioni rende difficile distinguere tra dati accurati e disinformazione. Inoltre, l'uso di tecnologie avanzate da parte di attori statali e non statali richiede un costante aggiornamento delle competenze e degli strumenti OSINT. Tuttavia, con l'integrazione di intelligenza artificiale e machine learning, l'OSINT è destinato a diventare sempre più sofisticato, offrendo analisi più precise e tempestive.