Numero 5 - giugno 2025

OSINT

L'OPEN SOURCE INTELLIGENCE NELLA GEOPOLITICA E NELL'ANALISI DEI CONFLITTI

MIRKO LAPI

INDICE

Mirko Lapi è Consulente e Formatore specializzato in Open Source Intelligence (OSINT), sicurezza delle informazioni e sviluppo del pensiero critico applicato ai processi decisionali. Ha prestato servizio nelle Forze Armate italiane per 27 anni, di cui 16 anni all'interno del II Reparto Informazioni e Sicurezza dello Stato Maggiore della Difesa, dove ha lavorato come analista presso il Centro Intelligence Interforze dello Stato Maggiore della Difesa e come docente di Intelligence presso il Centro Interforze di Formazione Intelligence (CIFIGE). È Professore a contratto di Open Source Intelligence (OSINT) presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Foggia. Inoltre, ricopre il ruolo di Professore a contratto di Cyber Security per il Corso di Laurea Magistrale in Ingegneria dei Sistemi Intelligenti presso la Facoltà di Ingegneria, Università Campus Bio-Medico di Roma.

Numero 5
giugno 2025

INTRODUZIONE

L'OSINT NEL'AMBITO DELL'INTELLIGENCE CONTEMPORANEA

L'Open Source Intelligence (OSINT) si è ormai affermata come una disciplina formale e centrale nel campo dell'Intelligence contemporanea. La sua essenza risiede nella ricerca, raccolta, elaborazione e analisi sistematica di dati e notizie provenienti da fonti aperte e pubblicamente accessibili, al fine di produrre conoscenza utile a supportare processi decisionali. Queste fonti comprendono un vasto spettro di informazioni, che spaziano dai media tradizionali (stampa, radio, televisione) alle risorse digitali (internet, social media, blog, forum), dai dati governativi pubblici (report, budget, audizioni) alle pubblicazioni accademiche e professionali, fino ai dati commerciali e alle immagini satellitari disponibili.

È fondamentale distinguere l'OSINT dalla mera ricerca o dalla semplice raccolta di informazioni. L'OSINT applica un rigoroso processo di Intelligence, strutturato e metodologico, per trasformare informazioni grezze, spesso frammentarie e non strutturate, in conoscenza raffinata e contestualizzata, specificamente orientata a soddisfare precise esigenze informative o a supportare decisioni specifiche di individui o

gruppi. Non si tratta quindi di una semplice ricerca su Google, ma di un'attività analitica che richiede competenze specifiche, strumenti dedicati e un approccio critico.

Il riconoscimento dell'OSINT come disciplina centrale è testimoniato dalla sua crescente integrazione accanto alle forme tradizionali di Intelligence come HUMINT (Human Intelligence), TECHINT (Technical Intelligence) e GEOINT (Geospatial Intelligence), ecc... Significativamente, l'*Office of the Director of National Intelligence* (ODNI) degli Stati Uniti ha recentemente definito l'OSINT come "l'INT di prima istanza" ("INT of first resort"), sottolineando il suo ruolo primario e fondamentale nel ciclo Intelligence moderno. Questa considerazione non deriva semplicemente dall'abbondanza di dati disponibili, ma riflette un cambiamento più profondo nel paradigma dell'Intelligence. L'enfasi crescente sull'OSINT è anche una risposta strategica ai limiti intrinseci, ai costi elevati e ai rischi associati ai metodi clandestini di raccolta tradizionali, specialmente in un'era caratterizzata da trasparenza e connettività digitale. L'OSINT offre un'alternativa o un complemento a basso rischio “e spesso più efficiente in termini di costi” per ottenere una comprensione fondamentale del contesto operativo.

Numero 5
giugno 2025

Tuttavia, la stessa definizione di OSINT non è monolitica e presenta sfumature in costante evoluzione. Mentre il nucleo si basa su informazioni "pubblicamente disponibili", alcune definizioni, ad esempio in ambito NATO, includono anche "altre informazioni non classificate che hanno una distribuzione pubblica o un accesso limitato". L'inclusione di dati commercialmente disponibili (CAI) e di informazioni con accesso ristretto sfuma ulteriormente i confini, suggerendo che l'OSINT sta espandendo il suo raggio d'azione anche oltre le fonti puramente "aperte" nel senso più stretto. Questo ampliamento aumenta l'utilità analitica dell'OSINT ma solleva anche nuove questioni etiche e di accessibilità.

LA CRESCENTE RILEVANZA DELL'OSINT NELLA GEOPOLITICA E NELL'ANALISI DEI CONFLITTI

Negli ultimi anni l'importanza dell'OSINT negli ambiti della Geopolitica e dell'analisi dei conflitti è cresciuta esponenzialmente, rendendo questa disciplina uno strumento sempre più indispensabile per analisti e decisori. Diversi fattori concomitanti spiegano questa acquisita centralità. In primo luogo, l'esplosione del volume di informazioni digitali generate e condivise quotidianamente ha creato un ecosistema informativo senza precedenti. Social media, blog, forum online, database pubblici,

Numero 5
giugno 2025

immagini satellitari commerciali e una miriade di altre fonti digitali offrono una quantità immensa di dati grezzi che, se analizzati correttamente, possono fornire informazioni rilevanti.

In secondo luogo, la natura stessa delle minacce e delle dinamiche globali è cambiata. Le minacce odierne sono spesso diffuse geograficamente, in rapida evoluzione e operano in ambienti informativi complessi, inclusa la cosiddetta "gray zone" (zona grigia), dove attori statali e non statali utilizzano tattiche ibride come campagne di disinformazione, operazioni informatiche e guerre per procura, spesso condotte apertamente. In questo contesto, l'OSINT diventa la prima linea di difesa per rilevare, attribuire e contrastare tali operazioni. La velocità con cui si sviluppano gli eventi richiede capacità di Intelligence tempestive e verificabili, caratteristiche intrinseche dell'OSINT.

Infine, l'OSINT dimostra una notevole versatilità ed è applicabile sia all'analisi strategica di lungo periodo sia al monitoraggio tattico di eventi dinamici. Da un lato, permette di comprendere tendenze geopolitiche, come le intenzioni strategiche degli stati, i cambiamenti nelle politiche economiche, le dinamiche commerciali globali e l'evoluzione dell'opinione pubblica.

Numero 5
giugno 2025

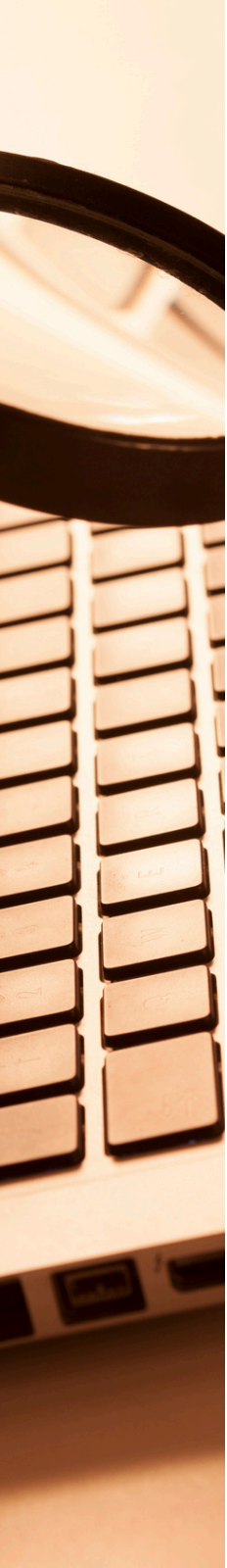
Dall'altro, si rivela importante anche per quanto attiene il monitoraggio dei movimenti militari, la verifica delle informazioni in tempo reale, la documentazione di potenziali crimini di guerra e il contrasto alla disinformazione.

STRUTTURA DELL'E-BOOK

Questo lavoro si propone di fornire una panoramica generale dell'utilità dell'OSINT nell'ambito della Geopolitica e dei conflitti. Inizieremo con l'esplorazione dei fondamenti concettuali dell'OSINT, inclusa la sua definizione, l'evoluzione storica, il ciclo di Intelligence applicato e la tassonomia delle fonti e delle metodologie di raccolta.

Successivamente, ci concentreremo sulle applicazioni specifiche dell'OSINT per l'analisi Geopolitica, esaminando come possa favorire la comprensione delle dinamiche statali, economiche e sociali a livello internazionale. Seguirà una disamina dettagliata del ruolo dell'OSINT nell'analisi dei conflitti contemporanei, con esempi concreti tratti da eventi recenti, mettendo in luce il contributo di attori non statali come Bellingcat. Valuteremo poi i vantaggi strategici e il valore aggiunto dell'OSINT rispetto ad altre discipline di Intelligence.

Analizzeremo altresì le sfide e le limitazioni intrinseche dell'OSINT, tra cui il sovraccarico informativo, i problemi della verifica, le questioni etiche e la questione delle risorse disponibili. Infine, esploreremo le traiettorie future dell'OSINT, con particolare attenzione all'impatto dell'Intelligenza Artificiale (IA), per concludere con una sintesi delle raccomandazioni strategiche per sfruttare efficacemente questo potente strumento di Intelligence. L'obiettivo è offrire un prodotto destinato a professionisti, ricercatori, studenti e appassionati del settore che consenta di comprendere questa disciplina che, già oggi, rappresenta un concreto vantaggio competitivo per chi la sa utilizzare e “governare”.



I FONDAMENTI DELL'OSINT

QUADRO CONCETTUALE: DEFINIZIONE, EVOLUZIONE E PRINCIPI FONDAMENTALI

L'Open Source Intelligence (OSINT) è formalmente definita come l'Intelligence prodotta a partire da informazioni pubblicamente disponibili (Publicly Available Information - PAI) o commercialmente disponibili (Commercially Available Information - CAI). Questo processo implica la raccolta, lo sfruttamento (analisi) e la disseminazione tempestiva di tali informazioni a un pubblico appropriato, al fine di rispondere a specifici requisiti o colmare lacune informative.

Diverse entità offrono ulteriori definizioni: il governo USA enfatizza la PAI e la tempestività per requisiti specifici; la NATO include anche informazioni non classificate con distribuzione o accesso limitato; l'Unione Europea e aziende private, come IBM e CrowdStrike, sottolineano la raccolta e l'analisi di PAI per generare Intelligence *actionable* a supporto della sicurezza nazionale, dell'applicazione della legge

Numero 5
giugno 2025

e della business Intelligence. In realtà la vera distinzione importante da tenere a mente è tra la semplice informazione open source e l'Intelligence derivata da essa attraverso un processo analitico strutturato.

EVOLUZIONE STORICA

Sebbene la pratica di utilizzare fonti aperte per scopi di Intelligence abbia radici antiche (si pensi alla Venezia rinascimentale o all'analisi sistematica di giornali avversari da parte degli Stati Maggiori nel XIX secolo), l'OSINT come disciplina formalizzata è un fenomeno più recente. Le sue origini moderne possono essere fatte risalire alla Seconda Guerra Mondiale con la creazione del *Foreign Broadcast Monitoring Service* (FBMS) negli Stati Uniti nel 1941, incaricato di monitorare le trasmissioni straniere.

Durante la Guerra Fredda, le fonti aperte (media stranieri, pubblicazioni tecniche) divennero una risorsa fondamentale, spesso "la fonte principale" per comprendere le capacità militari e le intenzioni politiche degli avversari, fornendo contesto e talvolta indicatori di preallarme. Il termine "OSINT" fu coniato dalle Forze Armate statunitensi alla fine degli anni '80 per rispondere alla natura dinamica dei requisiti informativi, specialmente a livello tattico.
L'*Intelligence Reorganization Ac*t del 1992 e la creazione del *Community Open Source Program Office* (COSPO) nel 1994 segnarono

Numero 5
giugno 2025

ulteriori passi verso l'istituzionalizzazione formale della disciplina. Tuttavia, sono stati l'avvento di Internet e la successiva esplosione dei social media a trasformare radicalmente l'OSINT. Infatti, eventi come la Rivoluzione Verde in Iran nel 2009 e le Primavere Arabe hanno dimostrato il potere delle informazioni generate dai cittadini e diffuse online.

In questo contesto, attori non statali, in particolare collettivi di giornalismo investigativo come Bellingcat, hanno svolto un ruolo pionieristico nello sviluppare e diffondere metodologie OSINT avanzate, spesso superando in agilità le strutture governative tradizionali. Questa evoluzione, da un monitoraggio prevalentemente passivo dei media, a un'indagine digitale attiva e analitica rappresenta un cambiamento qualitativo, che trasforma l'OSINT da semplice raccolta di notizie a generazione proattiva di Intelligence, spesso al di fuori dei canali istituzionali tradizionali.

PRINCIPI FONDAMENTALI

L'esercizio dell'OSINT si basa su alcuni principi cardine. Innanzitutto, la legalità e l'etica nella raccolta e nell'utilizzo delle informazioni: l'OSINT si distingue per l'uso di fonti apertamente e legalmente accessibili. Informazioni ottenute illegalmente, come leak di materiale classificato, non rientrano

Numero 5
giugno 2025

nella definizione di OSINT. Il focus primario è sulla produzione di *Intelligence actionable,* ovvero conoscenza elaborata e contestualizzata che supporta direttamente un processo decisionale o risponde a un'esigenza informativa specifica, distinguendola dalla ricerca accademica o dal giornalismo generico. Infine, centrale è il processo analitico: l'OSINT non è solo raccolta, ma implica valutazione critica delle fonti, analisi rigorosa dei dati, sintesi delle informazioni e produzione di giudizi ponderati.

IL CICLO DELL'INTELLIGENCE APPLICATO ALL'OSINT

A similitudine delle altre discipline di Intelligence, l'OSINT opera seguendo un ciclo strutturato, adattato alle specificità delle fonti aperte. Questo ciclo, sebbene concettualmente simile a quello tradizionale, presenta sfide uniche in ogni sua fase a causa della natura stessa dell'ambiente open source.

Pianificazione e Direzione (Planning & Direction) Questa fase iniziale definisce gli obiettivi dell'indagine OSINT. Si tratta di identificare chiaramente i requisiti informativi (cosa si deve sapere?), le entità di input (le informazioni di partenza, es. nome di una persona) e le entità di output desiderate (il risultato finale, es. eventuali affiliazioni).

Numero 5
giugno 2025

Una pianificazione accurata è fondamentale per focalizzare la ricerca ed evitare dispersioni.

Raccolta (Collection) È la fase di acquisizione delle informazioni grezze da una vasta gamma di fonti aperte identificate nella fase di pianificazione. Data l'eterogeneità e l'abbondanza delle fonti, questa fase richiede non solo la conoscenza delle fonti stesse, ma anche un'"Intelligence delle fonti", ovvero sapere chi possiede l'informazione necessaria o come accedervi. Le tecniche di raccolta, come vedremo, sono molteplici e variano a seconda dell'obiettivo. Tutte devono però seguire un comune denominatore: assicurarsi che la raccolta avvenga nel rispetto delle leggi sulla privacy e dei termini di servizio delle piattaforme.

Elaborazione (Processing) Le informazioni raccolte sono spesso voluminose, non strutturate, multilingue e di qualità variabile. In questa fase vengono quindi trasformate in un formato utilizzabile per l'analisi. L'elaborazione include attività come la traduzione, la trascrizione, il filtraggio del "rumore" (eliminazione del superfluo), la strutturazione dei dati, la decodifica di formati e la valutazione preliminare della pertinenza. Il sovraccarico informativo rappresenta una sfida significativa che richiede sempre più frequentemente strumenti automatizzati per la gestione dei dati.

Numero 5
giugno 2025

Analisi e Produzione (Analysis & Production)
Questo è il cuore del processo OSINT, dove le informazioni elaborate vengono trasformate in Intelligence. L'analista valuta criticamente l'affidabilità e la credibilità delle fonti e delle informazioni, identifica pattern, tendenze, connessioni e anomalie, confronta dati provenienti da fonti diverse (corroborazione), interpreta il significato nel contesto degli obiettivi e produce giudizi analitici. La sfida principale è la verifica dell'accuratezza in un ambiente saturo di disinformazione e potenziali manipolazioni. L'analisi richiede quindi pensiero critico, conoscenza del dominio e capacità di sintesi.

Disseminazione (Dissemination)
L'Intelligence prodotta viene confezionata in un formato appropriato (report, briefing, database, visualizzazioni) e distribuita tempestivamente ai decisori o agli utenti che l'hanno richiesta. La modalità di disseminazione deve tenere conto delle esigenze del destinatario e dell'eventuale necessità di proteggere le metodologie utilizzate, anche se le fonti sono aperte.

Valutazione e Feedback (Evaluation & Feedback) Questa fase, spesso trascurata, chiude il ciclo. Gli utenti dell'Intelligence forniscono un riscontro sull'utilità, la tempestività e l'accuratezza del prodotto ricevuto. Questo feedback è essenziale per

Numero 5
giugno 2025

affinare i requisiti, migliorare le tecniche di raccolta e analisi e rendere il processo OSINT più efficace nel tempo. L'OSINT è un processo intrinsecamente iterativo.

L'applicazione di questo ciclo all'OSINT evidenzia come le peculiarità dell'ambiente open source – volume, velocità, varietà, veridicità variabile – impattino criticamente ogni fase, richiedendo approcci e strumenti specifici rispetto alle discipline di Intelligence tradizionali.

TASSONOMIA DELLE FONTI APERTE E METODOLOGIE DI RACCOLTA

La forza dell'OSINT risiede nella vastità e diversità delle fonti a cui si può attingere. Una comprensione sistematica di queste fonti e delle relative tecniche di raccolta è essenziale per condurre indagini efficaci.

Categorie di Fonti Aperte

Le fonti OSINT possono essere classificate in diverse categorie principali:

- **Media:** Include fonti tradizionali come giornali, riviste, trasmissioni radiofoniche e televisive, sia nazionali che internazionali. Forniscono notizie, analisi e opinioni correnti.

Numero 5
giugno 2025

- **Internet**: La categoria più vasta e dinamica. Comprende siti web, pubblicazioni online, blog, forum di discussione, social media (Facebook, Twitter/X, LinkedIn, Instagram, TikTok, Telegram, ecc... - Social Media Intelligence o SOCMINT), contenuti generati dagli utenti (video su YouTube, post, commenti), archivi digitali, siti di notizie specializzate. La sua tempestività e facilità di accesso la rendono una fonte primaria.
- **Dati governativi pubblici**: Report ufficiali, budget, atti parlamentari, audizioni, elenchi telefonici, conferenze stampa, siti web istituzionali, discorsi pubblici, database demografici, registri pubblici (proprietà, imprese, tribunali). Fonti ufficiali ma accessibili pubblicamente.
- **Pubblicazioni professionali e accademiche**: Riviste scientifiche, atti di conferenze, simposi, paper accademici, tesi di laurea, dissertazioni, libri. Forniscono analisi approfondite, dati di ricerca e opinioni di esperti.
- **Dati commerciali:** Informazioni acquisite da data broker, database commerciali specializzati (es. finanziari, aziendali), immagini satellitari commerciali, dati di mercato, report di settore. Spesso richiedono un abbonamento o un acquisto.

Numero 5
giugno 2025

- **Letteratura grigia (Gray Literature):** Documenti come report tecnici, pre-print, tesi non pubblicate, documenti di lavoro, newsletter specialistiche, che non sono diffusi attraverso i canali editoriali commerciali tradizionali.
- **Dati geospaziali (GEOINT come OSINT):** Mappe pubbliche (es. OpenStreetMap), immagini satellitari commerciali o liberamente accessibili (es. Google Earth, Sentinel Hub, Zoom Earth), dati di geolocalizzazione derivati da altre fonti (es. metadati di foto, check-in sui social media).
- **Dark Web:** Contenuti presenti su reti overlay che richiedono software specifici per l'accesso (es. Tor). Può includere forum, marketplace illegali, siti di leak di dati. La raccolta nel Dark Web presenta rischi tecnici e legali aggiuntivi.
- **Identità digitale / Human footprint:** Tracce digitali lasciate dalle persone online, inclusi profili social, commenti, metadati, cronologie di attività.

Metodologie e tecniche di Raccolta

La raccolta di informazioni da queste fonti impiega una varietà di tecniche, spesso combinate tra loro e supportate da strumenti software specifici:

- **Ricerche avanzate sui motori di ricerca:** Utilizzo di operatori di ricerca specifici

(es. Google Dorking) per affinare le query e scoprire informazioni indicizzate ma non facilmente reperibili.

- **Monitoraggio e Analisi dei Social Media (SOCMINT)**: Tracciamento di profili, hashtag, parole chiave, discussioni, analisi di sentiment, identificazione di reti e influencer, rilevamento di bot e campagne coordinate.

- **Web scraping**: Utilizzo di software per estrarre automaticamente grandi quantità di dati da siti web. Richiede attenzione ai termini di servizio e considerazioni etiche/legali.

- **Analisi di metadati**: Estrazione di informazioni nascoste all'interno di file digitali (foto, video, documenti), come coordinate GPS, data/ora, tipo di dispositivo.

- **Analisi geospaziale (GEOINT)**: Utilizzo di piattaforme di mappatura e immagini satellitari per geolocalizzare eventi, verificare luoghi, monitorare cambiamenti nel tempo, analizzare infrastrutture o movimenti.

Numero 5
giugno 2025

- **Verifica di Registri pubblici**: Consultazione di database governativi o commerciali per informazioni su persone, aziende, proprietà, licenze.

- **Network Analysis**: Mappatura e analisi delle relazioni tra entità (persone, organizzazioni, siti web, ecc.) per identificare connessioni nascoste o strutture di influenza.

- **Ricerca nel Dark Web**: Utilizzo di motori di ricerca specifici per Tor (es. OnionScam) per esplorare contenuti non indicizzati sul web di superficie.

- **Utilizzo di strumenti specializzati:** Impiego di piattaforme software dedicate all'OSINT che aggregano fonti, automatizzano ricerche e facilitano l'analisi e la visualizzazione.

È importante notare che l'efficacia dell'OSINT spesso deriva dalla capacità di integrare informazioni provenienti da diverse categorie di fonti e dall'applicazione combinata di molteplici tecniche. Inoltre, la crescente disponibilità di fonti tradizionalmente associate ad altre discipline INT (come GEOINT commerciale o dati su

segnali RF disponibili pubblicamente) sta rendendo l'analista OSINT una figura sempre più multidisciplinare, richiedendo competenze che vanno ben oltre la semplice ricerca online.
Questa convergenza amplia le potenzialità dell'OSINT, ma ne aumenta anche la complessità.

L'OSINT COME STRUMENTO GEOPOLITICO

L'Open Source Intelligence si rivela uno strumento di straordinaria potenza per analizzare e comprendere le complesse dinamiche della Geopolitica contemporanea. La sua capacità di attingere a un'ampia gamma di informazioni pubblicamente disponibili consente di monitorare le azioni degli Stati, analizzare le tendenze economiche globali, valutare il sentimento pubblico e supportare le decisioni strategiche.

MONITORAGGIO DELLE STRATEGIE E DELLE DINAMICHE INTERNAZIONALI

L'OSINT offre finestre uniche sulle strategie e sulle azioni degli attori statali che caratterizzano la scena internazionale. Uno degli ambiti più evidenti è il monitoraggio delle capacità e delle attività militari. Attraverso l'analisi di immagini satellitari commerciali (GEOINT utilizzata come OSINT), post sui social media (foto e video condivisi da soldati o civili), dati sui trasporti (ferroviari, marittimi, aerei) e notizie locali, è possibile tracciare l'afflusso di forze militari, i movimenti di truppe e attrezzature, e lo svolgimento di esercitazioni.

L'analisi di questi indicatori, specialmente dei cambiamenti nella disposizione e nella forza delle unità militari, può fornire indizi importanti sulle possibili intenzioni di uno Stato, come dimostrato ampiamente nel periodo precedente l'invasione russa dell'Ucraina nel 2022, quando numerosi analisti OSINT documentarono il massiccio dispiegamento di forze russe ai confini.

Oltre all'aspetto militare, l'OSINT permette di analizzare le comunicazioni ufficiali e le attività diplomatiche. Discorsi di leader politici, comunicati stampa, report governativi, atti parlamentari, siti web istituzionali e resoconti di incontri diplomatici sono fonti aperte utilissime per comprendere le posizioni ufficiali, le strategie nazionali dichiarate e le direzioni della politica estera. Monitorare i sottili cambiamenti nelle politiche governative, negli investimenti strategici, nelle nuove leggi o nei trattati commerciali può aiutare a inferire anche intenzioni strategiche a lungo termine.

Un altro rilevante campo di applicazione è il **monitoraggio delle attività informatiche sponsorizzate da Stati e delle campagne di influenza**. L'OSINT è fondamentale per identificare e analizzare campagne di disinformazione, propaganda e operazioni psicologiche condotte attraverso i media digitali per plasmare le percezioni pubbliche,

destabilizzare avversari o promuovere specifici interessi geopolitici. L'analisi del traffico IP, delle registrazioni di domini, delle sessioni web e dei database trapelati può contribuire a determinare l'attribuzione di attacchi informatici.

Infine, l'OSINT consente di valutare la stabilità politica interna monitorando eventi come proteste, disordini sociali, elezioni e dinamiche di leadership attraverso notizie locali, social media e report di ONG. Questa analisi fornisce un contesto essenziale per comprendere la capacità di uno stato di agire sulla scena internazionale e le potenziali vulnerabilità interne.

ANALISI DEGLI INDICATORI ECONOMICI E DEI FLUSSI COMMERCIALI GLOBALI

Le dinamiche economiche sono intrinsecamente legate alla Geopolitica e l'OSINT offre strumenti potenti per monitorarle. È infatti possibile seguire le tendenze economiche generali, il sentiment di mercato e le notizie finanziarie attraverso portali specializzati, report aziendali, pubblicazioni accademiche e discussioni online, per valutare la salute economica di una Nazione, identificare settori in crescita o in crisi e rilevare potenziali vulnerabilità economiche che potrebbero avere implicazioni geopolitiche.

L'OSINT è particolarmente efficace nel tracciare i flussi commerciali globali e le dinamiche delle catene di approvvigionamento. Utilizzando dati PAI e CAI, come i dati di tracciamento delle navi (es. AIS - Automatic Identification System, monitorabile tramite piattaforme come MarineTraffic), attività portuale, dati doganali e immagini satellitari, gli analisti possono mappare le rotte commerciali, identificare colli di bottiglia, monitorare il commercio di specifiche materie prime e rilevare cambiamenti nei pattern commerciali che possono segnalare spostamenti geopolitici o tensioni economiche.

Un'applicazione specifica di grande rilevanza è il **monitoraggio dell'applicazione delle sanzioni economiche e l'identificazione di tattiche di evasione**. L'analisi dei movimenti navali sospetti (es. spegnimento dei transponder AIS, trasferimenti da nave a nave in acque neutre), l'incrocio con registri societari per identificare società di comodo e l'uso di immagini satellitari per verificare attività portuali non autorizzate sono tecniche OSINT utilizzate per smascherare tentativi di aggirare le sanzioni internazionali. Piattaforme come Trade Map forniscono statistiche commerciali dettagliate che possono essere analizzate per valutare l'impatto delle sanzioni.

Inoltre, l'OSINT può contribuire all'**analisi della Geopolitica dell'energia**, monitorando la produzione, il trasporto e il consumo di risorse energetiche, le politiche energetiche nazionali, gli investimenti in infrastrutture e le dichiarazioni pubbliche relative alla sicurezza energetica, un fattore chiave nelle relazioni internazionali. Il monitoraggio di questi indicatori economici e commerciali fornisce una comprensione granulare dell'intersezione tra economia e politica globale, consentendo di anticipare instabilità e cambiamenti nelle alleanze.

VALUTAZIONE DEL SENTIMENTO PUBBLICO E CONTRASTO ALLE OPERAZIONI DI INFLUENZA

Comprendere l'opinione pubblica all'interno di diverse Nazioni e a livello transnazionale è un aspetto fondamentale nell'analisi Geopolitica e l'OSINT offre metodi per farlo anche su larga scala. Attraverso il monitoraggio dei social media e l'analisi del sentiment, è possibile misurare le reazioni pubbliche a politiche governative, eventi internazionali, figure politiche o crisi in corso. Tecniche come l'analisi del linguaggio naturale (NLP) e l'apprendimento automatico (Machine Learning) vengono sempre più utilizzate per processare grandi volumi di testo e identificare tendenze,

polarizzazione e narrazioni dominanti all'interno di specifiche popolazioni o gruppi online. Ciò può rivelare il livello di supporto pubblico per determinate politiche, potenziali instabilità sociali o l'efficacia della propaganda.

Strettamente collegato è il ruolo dell'OSINT nell'**identificare, analizzare e contrastare le campagne di disinformazione e propaganda**. Gli analisti OSINT utilizzano tecniche come l'analisi delle reti sociali per mappare la diffusione di narrazioni specifiche, l'identificazione di account bot o coordinati (inauthentic behavior), il tracciamento dell'origine di contenuti manipolati (deepfake, immagini fuorvianti) e la verifica dei fatti (fact-checking) per smascherare operazioni di influenza ostili. Comprendere come vengono costruite e diffuse queste campagne è essenziale per sviluppare contromisure efficaci e proteggere il dibattito pubblico.

Infine, l'OSINT aiuta a **comprendere le sfumature culturali e le tendenze sociali** che sottendono gli sviluppi politici. L'analisi di contenuti culturali, discussioni online, report antropologici o sociologici disponibili pubblicamente può fornire un contesto prezioso per interpretare eventi politici e sociali, evitando analisi superficiali o etnocentriche.

Tuttavia, è proprio la natura pubblica dell'OSINT a renderla un'arma a doppio taglio in questo dominio. Mentre è uno strumento potente per smascherare la disinformazione, l'ambiente informativo open source è esso stesso il campo di battaglia dove queste campagne informative vengono combattute. Attori statali e non statali non solo diffondono disinformazione, ma possono anche tentare attivamente di "intossicare" le fonti aperte per ingannare gli analisti OSINT. Questo crea una dinamica competitiva costante tra chi cerca di verificare l'informazione e chi cerca di manipolarla, rendendo la validazione critica e la consapevolezza delle tecniche di inganno elementi essenziali dell'analisi OSINT applicata alla Geopolitica.

INFORMARE LA POLITICA STRATEGICA E IL PROCESSO DECISIONALE

L'OSINT svolge un ruolo sempre più centrale nell'informare la politica estera e di sicurezza e nel supportare il processo decisionale a livello strategico. Consente infatti di fornire Intelligence fondamentale e consapevolezza situazionale (situational awareness) ai policy-maker, offrendo una base di conoscenza sul contesto operativo, sulle capacità degli attori e sulle tendenze emergenti.

Numero 5
giugno 2025

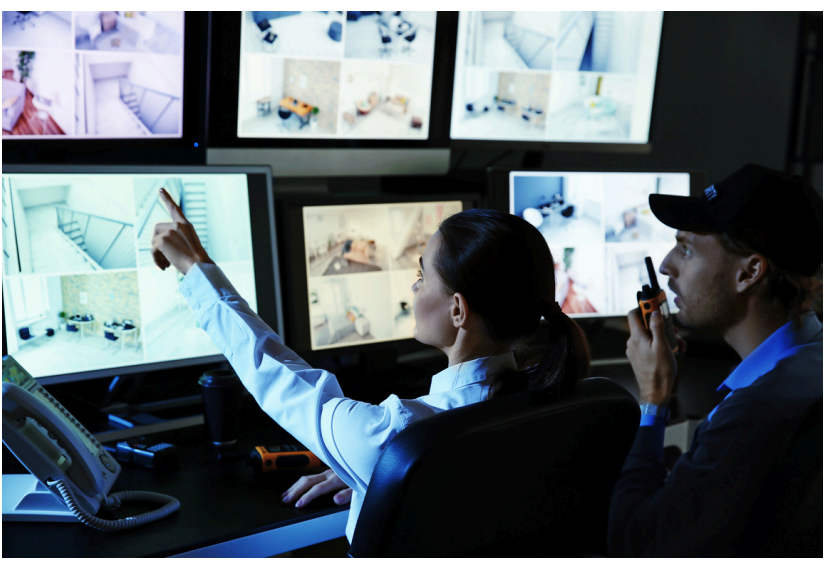
La sua capacità di fornire rapidamente una comprensione aggiornata dell'ambiente operativo è particolarmente utile soprattutto in situazioni di crisi o in rapida evoluzione. Un vantaggio chiave è la sua condivisibilità. Poiché deriva da fonti aperte, l'Intelligence OSINT può spesso essere condivisa più ampiamente, sia all'interno delle Istituzioni sia con partner internazionali o con il pubblico, senza compromettere fonti o metodi classificati. Ciò facilita la collaborazione, supporta gli sforzi diplomatici fornendo informazioni verificabili e può essere utilizzata per giustificare pubblicamente decisioni politiche.

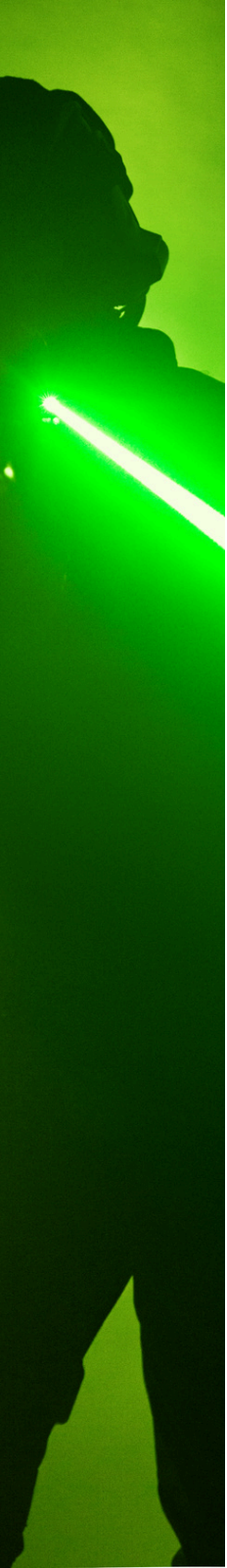
La **NATO**, ad esempio, riconosce esplicitamente il potenziale dell'OSINT e sta sviluppando capacità dedicate. Per l'Alleanza, l'OSINT è utile per comprendere l'ambiente informativo, informare il processo decisionale, monitorare le intenzioni degli avversari, identificare e contrastare campagne di disinformazione e integrare altre discipline di Intelligence come l'IMINT (Imagery Intelligence) per produrre Intelligence "*all source*" e *actionable*. La NATO mira a un sistema OSINT olistico che combini analisti addestrati (persone), processi standardizzati e strumenti potenti su una piattaforma digitale comune, abilitata da diverse fonti di dati. L'obiettivo è migliorare la situational awareness e la reattività

Numero 5
giugno 2025

dell'Alleanza attraverso un input tempestivo per gli indicatori e gli avvertimenti (Indications and Warnings - I&W).

Più in generale, i **governi** utilizzano ampiamente l'OSINT per una varietà di scopi, tra cui la sicurezza nazionale, l'antiterrorismo, la protezione delle infrastrutture critiche, la comprensione di culture straniere e il supporto alle operazioni militari. La capacità dell'OSINT di fornire un monitoraggio continuo e quasi in tempo reale di indicatori geopolitici (militari, economici, sociali) su vasta scala rappresenta un cambiamento significativo rispetto alle valutazioni periodiche basate principalmente su fonti classificate e consente una consapevolezza situazionale più dinamica e persistente.





L'APPLICAZIONE DELL'OSINT NEI CONFLITTI CONTEMPORANEI

Nei teatri di conflitto moderni, caratterizzati da flussi informativi rapidi, accesso spesso limitato e guerra dell'informazione pervasiva, l'OSINT è diventato uno strumento indispensabile per l'analisi, la verifica e la documentazione degli eventi.

CONSAPEVOLEZZA DEL CAMPO DI BATTAGLIA IN TEMPO REALE E ANALISI MILITARE

L'OSINT fornisce capacità senza precedenti per monitorare e analizzare le operazioni militari quasi in tempo reale. Attraverso la raccolta e l'analisi di immagini satellitari commerciali, video e fotografie condivise sui social media da soldati e civili, dati di tracciamento dei trasporti e notizie locali, è possibile seguire i movimenti delle truppe, il dispiegamento di equipaggiamenti specifici (come pontoni per attraversamenti fluviali o sistemi missilistici), le preparazioni logistiche (come la creazione di ospedali da campo o scorte di sangue) e l'andamento generale delle operazioni. L'ammassamento di forze russe prima dell'invasione dell'Ucraina nel 2022 è stato ampiamente documentato tramite attività OSINT,

fornendo indicatori anticipati dell'imminenza del conflitto.

L'OSINT permette anche di **valutare i danni sul campo di battaglia**, sia alle infrastrutture civili sia agli equipaggiamenti militari. Progetti come quello del blog Oryx, che ha meticolosamente documentato le perdite di equipaggiamento russo e ucraino basandosi su prove visive open source, dimostrano la potenza di questo approccio. L'analisi di immagini satellitari pre e post attacco consente di valutare l'estensione dei danni a edifici, ponti o basi militari.

Analizzando le azioni osservate attraverso fonti aperte, è possibile inoltre **dedurre tattiche, tecniche e procedure (TTPs)** utilizzate dalle forze in campo, comprendendo meglio le loro dottrine operative e le loro capacità. L'OSINT può essere rilevante anche per **identificare specifiche unità militari o sistemi d'arma** coinvolti in particolari incidenti. Ad esempio, l'analisi meticolosa di foto e video ha permesso a Bellingcat e ad altri ricercatori di identificare il lanciamissili Buk specifico ritenuto responsabile dell'abbattimento del volo MH17 nel 2014. Allo stesso modo, l'analisi dei resti di munizioni può aiutare a identificare il tipo di arma utilizzata e, potenzialmente, la sua origine.

Numero 5
giugno 2025

Infine, l'uso di **dati geospaziali open source (GEOINT)** è fondamentale per l'analisi militare. Piattaforme come Google Earth, OpenStreetMap e immagini satellitari commerciali sono utilizzate per creare mappe aggiornate, analizzare il terreno e la sua percorribilità, valutare la visibilità, identificare potenziali bersagli o posizioni difensive e geolocalizzare eventi.

VERIFICA, FACT-CHECKING E CONTRASTO ALLA DISINFORMAZIONE IN GUERRA

L'ambiente informativo durante un conflitto è notoriamente caotico e soggetto a manipolazioni ("*fog of war*"). L'OSINT fornisce strumenti essenziali per navigare questa complessità, verificare le informazioni e contrastare la disinformazione. Una delle applicazioni più importanti è la verifica di contenuti generati dagli utenti (*User-Generated Content* - UGC), come foto e video provenienti dalle zone di conflitto.
Gli analisti OSINT utilizzano tecniche di **geolocalizzazione** (determinare dove è stata scattata una foto/video confrontando elementi visivi come edifici, montagne, minareti con immagini satellitari o mappe) e **cronolocalizzazione** (determinare quando è stata scattata, analizzando ombre, condizioni meteorologiche, metadati o confrontando con altri eventi noti) per confermare l'autenticità e il contesto del materiale.

Numero 5
giugno 2025

Questa capacità di verifica è fondamentale per **smascherare la disinformazione e la propaganda** diffuse da tutte le parti in conflitto. L'OSINT permette di identificare narrazioni false, filmati decontestualizzati o manipolati (inclusi i deepfake), eventi inscenati o attribuzioni errate di responsabilità. Ad esempio, durante il conflitto siriano, l'OSINT è stato utilizzato per smentire le affermazioni del Governo siriano riguardo all'uso di armi chimiche.

In contesti dove l'accesso per i giornalisti tradizionali è limitato o pericoloso, l'OSINT diventa spesso la **principale forma di raccolta e verifica delle informazioni**, agendo come un "complemento fondamentale" e una "lente aggiuntiva" per corroborare le testimonianze provenienti dal terreno. Permette di incrociare e validare le affermazioni provenienti da fonti ufficiali, testimoni oculari o resoconti mediatici.

Numero 5
giugno 2025

DOCUMENTARE LE ATROCITÀ: OSINT NEL CONTESTO DEI CRIMINI DI GUERRA

L'OSINT ha assunto un ruolo sempre più importante anche nella **raccolta e conservazione di prove digitali relative a potenziali crimini di guerra**, violazioni dei diritti umani e del diritto internazionale umanitario. Video, fotografie, immagini satellitari, post sui social media e testimonianze digitali vengono sistematicamente raccolti, verificati (tramite geolocalizzazione, cronolocalizzazione, analisi dei metadati) e archiviati da organizzazioni specializzate (come Syrian Archive 56, Mnemonic, Eyes on Russia) e gruppi investigativi.

Queste prove open source possono essere utilizzate per **documentare specifici incidenti**, come attacchi contro civili o infrastrutture civili (ospedali, scuole), esecuzioni sommarie, torture, deportazioni forzate, uso di armi proibite (come armi chimiche in Siria) o saccheggio di risorse. L'analisi OSINT mira a **identificare gli autori** (analizzando uniformi, insegne, lingua parlata, armamenti), le **vittime**, i **luoghi** e le **date** precise degli eventi, nonché le **munizioni** o i metodi utilizzati.

L'obiettivo finale è supportare i processi di giustizia e accountability, fornendo materiale probatorio a organismi internazionali come la Corte Penale Internazionale (CPI), commissioni d'inchiesta delle Nazioni Unite o tribunali nazionali che esercitano giurisdizione universale. L'OSINT si rivela particolarmente utile soprattutto per documentare crimini commessi in aree occupate o inaccessibili agli investigatori sul campo. Tuttavia, l'ammissibilità delle prove OSINT nei procedimenti giudiziari è ancora un'area in evoluzione, che richiede metodologie rigorose e conformi agli standard probatori (vds il Berkeley Protocol) per garantire l'autenticità, l'integrità e la catena di custodia delle prove digitali.

IL RUOLO DEGLI ATTORI NON STATALI

È impossibile discutere dell'applicazione dell'OSINT nei conflitti senza riconoscere il ruolo pionieristico e l'impatto significativo di gruppi investigativi indipendenti, primo fra tutti Bellingcat. Fondato nel 2014 da Eliot Higgins, Bellingcat ha dimostrato come individui e piccoli gruppi, armati di metodologie OSINT rigorose e strumenti digitali, possano condurre indagini complesse su questioni di rilevanza globale, spesso sfidando le narrazioni ufficiali degli Stati.

Le **metodologie** impiegate da Bellingcat e gruppi simili includono una combinazione

sofisticata di geolocalizzazione e cronolocalizzazione di video e foto, analisi approfondita di immagini satellitari, monitoraggio dei social media, data mining di database pubblici e trapelati, analisi forense digitale, crowdsourcing per la raccolta e la verifica delle informazioni, e una forte enfasi sulla trasparenza metodologica. Spesso utilizzano il termine "*open-source investigation*" per sottolineare il processo investigativo e distinguersi dalle pratiche di Intelligence governative.

Le **indagini chiave** di Bellingcat che hanno avuto un impatto significativo sulla comprensione di conflitti e questioni geopolitiche includono:

- l'identificazione del sistema missilistico Buk russo e dell'unità militare responsabile dell'abbattimento del volo **MH17** sull'Ucraina nel 2014;
- la documentazione dell'uso di **armi chimiche** da parte del regime siriano;
- l'analisi dettagliata della **guerra in Ucraina**, inclusa la documentazione di crimini di guerra;
- l'indagine sui **crimini di guerra in Etiopia** durante il conflitto nel Tigray.

L'impatto di questi gruppi è molteplice: hanno dimostrato la capacità di smascherare narrazioni e operazioni coperte; hanno influenzato l'opinione pubblica e le decisioni politiche fornendo prove concrete e verificabili; hanno contribuito significativamente agli sforzi di accountability per gravi violazioni dei diritti umani; e hanno creato una sorta di "democratizzazione" delle capacità investigative, rendendo accessibili metodologie potenti a giornalisti, ricercatori e cittadini. Nonostante ciò, questi gruppi non sono esenti da critiche perché talvolta accusati di parzialità o di fare affidamento eccessivo su fonti digitali.

Il successo di attori come Bellingcat evidenzia comunque una trasformazione nel panorama informativo globale. Dimostra che capacità investigative precedentemente appannaggio quasi esclusivo degli Stati possono essere replicate da attori non statali, creando nuove dinamiche di potere informativo. Questa "democratizzazione" apparente, tuttavia, introduce anche attori che operano al di fuori dei tradizionali meccanismi di controllo statale, sollevando interrogativi sulla loro stessa accountability. Inoltre, la crescente complessità e il costo degli strumenti OSINT più avanzati in futuro potrebbero limitare questa democratizzazione.

Numero 5
giugno 2025

L'applicazione dell'OSINT nei conflitti ha anche reso più sfumati i confini tradizionali tra combattenti e civili, tra giornalisti e analisti e tra raccolta di Intelligence e informazione pubblica. I civili, attraverso i loro smartphone e account social, diventano sensori attivi sul campo di battaglia, contribuendo involontariamente (o talvolta volontariamente) all'Intelligence. I giornalisti adottano tecniche analitiche sofisticate, mentre gruppi OSINT agiscono quasi come “agenzie di Intelligence” private. Questa convergenza crea nuove opportunità ma anche nuove vulnerabilità e sfide etiche nella gestione dell'informazione in tempo di guerra.

VANTAGGI STRATEGICI DELL'OSINT

L'OSINT offre una serie di vantaggi distinti che ne giustificano la crescente importanza e il suo status di "INT di prima istanza" nel panorama dell'Intelligence moderna. Questi vantaggi spaziano da benefici operativi tangibili a contributi strategici più ampi.

BENEFICI OPERATIVI: TEMPESTIVITÀ, EFFICIENZA DEI COSTI E ACCESSIBILITÀ

- **Tempestività**: Uno dei principali punti di forza dell'OSINT è la sua capacità di fornire accesso a informazioni in tempo reale o quasi reale, specialmente attraverso fonti come i social media e le notizie online. Questa immediatezza è fondamenale in ambienti dinamici come crisi geopolitiche o conflitti armati, dove la velocità dell'informazione può fare la differenza, consentendo analisi e decisioni più rapide.

- **Efficienza dei costi:** Rispetto alle discipline di Intelligence classificate, che richiedono investimenti significativi in personale specializzato, addestramento, tecnologia sofisticata e operazioni

potenzialmente rischiose, l'OSINT è generalmente molto più efficiente dal punto di vista dei costi. Si basa in gran parte su risorse pubblicamente disponibili o su dati commerciali a basso costo, rendendo l'Intelligence di alta qualità più accessibile anche a organizzazioni con budget limitati.

- **Accessibilità**: Le fonti OSINT sono, per definizione, aperte e accessibili senza la necessità di autorizzazioni di sicurezza classificate o infrastrutture complesse. Questo, come detto, democratizza l'accesso all'informazione e permette a una gamma più ampia di analisti e organizzazioni (governative, non governative, accademiche, private) di partecipare alla raccolta e all'analisi di Intelligence.

- **Scalabilità**: Data la vastità dell'universo informativo open source, le operazioni OSINT possono essere potenzialmente scalate per coprire aree geografiche ampie o una molteplicità di argomenti in modo più flessibile rispetto a metodi di raccolta più mirati e *resource-intensive*.

Tuttavia, questa accessibilità e questo basso costo rappresentano anche un'arma a doppio taglio. Se da un lato permettono ad attori legittimi con risorse limitate (come ONG o giornalisti investigativi) di svolgere un lavoro

importante, dall'altro abbassano la barriera d'ingresso anche ad attori malintenzionati. Terroristi, gruppi criminali, Stati ostili e persino singoli individui possono utilizzare le stesse tecniche e fonti OSINT per condurre ricognizioni, pianificare attacchi, rubare identità o condurre spionaggio industriale, sfruttando la stessa facilità di accesso all'informazione. Questa simmetria nell'accessibilità è una caratteristica fondamentale e una vulnerabilità intrinseca dell'ecosistema OSINT.

COSTRUIRE CREDIBILITÀ ATTRAVERSO TRASPARENZA E VERIFICABILITÀ

A differenza dell'Intelligence classificata, i risultati dell'OSINT possono spesso essere verificati e controllati in modo indipendente da terze parti, come giornalisti, ricercatori o il pubblico stesso, poiché le fonti sottostanti sono aperte. Questa potenziale verificabilità conferisce all'OSINT un grado unico di trasparenza.

Questa trasparenza può essere utilizzata strategicamente per **costruire fiducia e credibilità** con diversi stakeholder, inclusi i decisori politici, i partner internazionali e l'opinione pubblica. In un'epoca di diffusa disinformazione, poter basare affermazioni o decisioni su prove apertamente verificabili è un vantaggio significativo.

Numero 5
giugno 2025

Inoltre, l'OSINT permette alle agenzie di Intelligence o ai governi di difendere pubblicamente i propri giudizi o le proprie azioni citando fonti aperte, senza dover rivelare o compromettere fonti e metodi classificati più sensibili. Questa capacità è particolarmente utile per comunicare con partner stranieri o per spiegare le motivazioni di determinate scelte politiche al pubblico. La verificabilità intrinseca dell'OSINT lo posiziona quindi come uno strumento potenziale per promuovere la fiducia e la cooperazione internazionale nel campo dell'Intelligence, consentendo discussioni più aperte rispetto a quelle basate esclusivamente su informazioni segrete.

SINERGIA CON LE DISCIPLINE DI INTELLIGENCE CLASSIFICATE

L'OSINT non sostituisce le discipline di Intelligence tradizionali, ma piuttosto le complementa e le potenzia in un approccio "all-source". Uno dei ruoli più importanti dell'OSINT è fornire il contesto fondamentale e la conoscenza di base ("80% baseline") su un determinato argomento o area geografica. Ciò permette alle risorse di raccolta classificate, che sono più costose, rischiose e limitate, di concentrarsi in modo mirato sulla raccolta di informazioni specifiche e critiche che non sono disponibili pubblicamente, colmando cosi le lacune informative.

L'OSINT può anche guidare e "indirizzare" altri metodi di raccolta, suggerendo dove dirigere satelliti spia, intercettazioni di segnali o agenti umani per ottenere le informazioni più cruciali. Inoltre, le informazioni provenienti da fonti aperte possono essere utilizzate per corroborare, validare o contestualizzare i dati ottenuti tramite mezzi classificati, aumentando la fiducia complessiva nel quadro di Intelligence prodotto. La NATO, ad esempio, enfatizza fortemente l'integrazione dell'OSINT con altre discipline come l'IMINT.

In alcuni casi, specialmente per certi argomenti (es. opinione pubblica, tendenze culturali) o in aree geografiche con limitata copertura da parte dei sistemi di raccolta classificati, l'OSINT può essere l'**unica fonte di informazione disponibile**. Il concetto che l'OSINT fornisca la "baseline dell'80%" suggerisce una riconsiderazione fondamentale del valore aggiunto della costosa raccolta classificata. Implica che gli investimenti futuri potrebbero orientarsi maggiormente verso l'ottimizzazione della sinergia tra Intelligence aperta e segreta, piuttosto che concentrarsi esclusivamente su quest'ultima. Le risorse classificate potrebbero diventare strumenti altamente mirati per colmare lacune specifiche e critiche identificate proprio grazie all'analisi

OSINT, modificando potenzialmente l'allocazione delle risorse all'interno delle comunità di Intelligence.

MITIGAZIONE DEL RISCHIO NELLE OPERAZIONI DI INTELLIGENCE

L'utilizzo dell'OSINT comporta intrinsecamente un rischio operativo inferiore rispetto ai metodi clandestini. La raccolta di informazioni da fonti aperte non richiede di mettere a rischio personale sul campo come ad esempio nella HUMINT.

Dal punto di vista **legale ed etico**, l'OSINT presenta generalmente meno rischi rispetto alla raccolta segreta, a condizione che gli analisti operino nel rispetto delle leggi sulla privacy, dei termini di servizio delle piattaforme e delle linee guida etiche. Non implica intrusioni o attività coperte, riducendo l'esposizione a contestazioni legali o a danni reputazionali.

Infine, come già accennato, l'OSINT può contribuire a **proteggere fonti e metodi classificati** più sensibili, permettendo di attribuire pubblicamente determinate scoperte o valutazioni a informazioni open source, anche quando queste sono state corroborate o inizialmente suggerite da canali segreti.

TABELLA 1: ANALISI COMPARATIVA DELLE DISCIPLINE DI INTELLIGENCE (1/2)

Disciplina	Caratteristiche Chiave (Fonti/Metodi)	Costo Relativo	Tempestività Relativa	Accessibilità Relativa	Rischio Operativo/Legale Relativo	Verificabilità Indipendente	Limitazioni Chiave
OSINT	Informazioni pubbliche/commerciali (media, web, social, record, GEOINT...)	Basso	Alta/Molto Alta	Alta	Basso	Alta/Media	Volume, Affidabilità, Disinformazione, Etica/Privacy, Necessità di competenze/tool
HUMINT	Informazioni da fonti umane (agenti, informatori, interrogatori)	Molto Alto	Variabile	Molto Bassa	Molto Alto	Molto Bassa	Rischio per le fonti, Accesso limitato, Possibile inganno, Lentezza
SIGINT	Intercettazione di segnali (comunicazioni elettroniche, segnali radar...)	Molto Alto	Alta	Molto Bassa	Alto	Molto Bassa	Crittografia, Volume dati, Costo tecnologia, Aspetti legali/sovranità

Numero 5
giugno 2025

TABELLA 1: ANALISI COMPARATIVA DELLE DISCIPLINE DI INTELLIGENCE (2/2)

Disciplina	Caratteristiche Chiave (Fonti/Metodi)	Costo Relativo	Tempestività Relativa	Accessibilità Relativa	Rischio Operativo/Legale Relativo	Verificabilità Indipendente	Limitazioni Chiave
GEOINT	Sfruttamento e analisi di immagini e informazioni geospaziali (satelliti...)	Alto/Molto Alto	Media/Alta	Bassa (classificata)	Medio/Alto	Bassa (classificata)	Copertura nuvolosa (ottica), Risoluzione, Costo asset, Analisi complessa
MASINT	Misurazione e analisi di firme e caratteristiche distintive di target	Molto Alto	Variabile	Molto Bassa	Alto	Molto Bassa	Necessità di sensori specifici, Complessità analisi, Interpretazione difficile

Numero 5
giugno 2025

Nota: La tabella presenta una valutazione relativa e qualitativa basata sulle fonti fornite. GEOINT commerciale/pubblico è considerato parte delle fonti OSINT.

Questa tabella riassume visivamente i punti di forza e di debolezza dell'OSINT rispetto alle discipline tradizionali, evidenziando perché sia considerata una componente fondamentale e spesso iniziale del processo di Intelligence moderno.

SFIDE E LIMITAZIONI DELL'OSINT

Nonostante i suoi indubbi vantaggi, l'OSINT presenta una serie di sfide e limitazioni intrinseche che devono essere comprese e gestite per garantirne un utilizzo efficace e responsabile. Queste sfide riguardano la gestione dei dati, la verifica dell'accuratezza, le considerazioni etiche e le risorse necessarie.

GESTIRE IL SOVRACCARICO INFORMATIVO

La caratteristica più evidente dell'ambiente open source è l'immensa quantità di dati disponibili. Il volume, la velocità e la varietà delle informazioni generate quotidianamente (si parla di zettabyte di dati) possono facilmente sopraffare le capacità di raccolta, elaborazione e analisi, sia umane che tecnologiche. Questo fenomeno, noto come *information overload*, rappresenta una sfida costante.

La difficoltà principale risiede nel **filtrare le informazioni rilevanti ("segnali") dal rumore di fondo**. Senza efficaci strategie e strumenti per la selezione, l'aggregazione e la prioritizzazione dei dati, gli analisti rischiano di perdere tempo su informazioni irrilevanti o, peggio, di non riuscire a identificare

informazioni critiche sepolte nella massa di dati. La gestione di questo sovraccarivo informativo richiede non solo strumenti tecnologici avanzati (come l'IA per l'automazione), ma anche metodologie analitiche rigorose e una chiara definizione degli obiettivi informativi.

GARANTIRE L'ACCURATEZZA

Forse la sfida più critica per l'OSINT è garantire l'accuratezza e l'affidabilità delle informazioni raccolte. Le fonti aperte sono intrinsecamente eterogenee in termini di qualità: possono essere incomplete, imprecise, datate, affette da bias (pregiudizi) o deliberatamente false.

- **Sfida della verifica**: La validazione dell'autenticità e della credibilità delle informazioni è un processo complesso e dispendioso in termini di tempo. Richiede un approccio critico e metodico, basato sulla corroborazione incrociata tra multiple fonti indipendenti, sulla valutazione della reputazione e dell'expertise della fonte originaria, sull'analisi del contesto e sulla ricerca di eventuali incongruenze. Non si può fare affidamento su una singola fonte.

- **Disinformazione e Inganno**: L'ambiente open source è un terreno fertile per la disinformazione (informazioni false

create e diffuse deliberatamente per ingannare) e la misinformazione (informazioni false diffuse senza intento malevolo). Attori statali e non statali utilizzano attivamente la propaganda, le fake news, i deepfake e altre tecniche di manipolazione per influenzare le percezioni, screditare avversari o nascondere le proprie attività. Le fonti aperte sono particolarmente vulnerabili all'"intossicazione", ovvero all'infiltrazione deliberata di informazioni false.

- **Contro-OSINT e inganno strategico**: Gli avversari consapevoli di essere monitorati tramite OSINT possono adottare misure attive per ingannare gli analisti (contro-OSINT). Questo può includere la diffusione mirata di informazioni fuorvianti, la manipolazione delle proprie tracce digitali, l'uso di proxy o false flag per nascondere la propria identità, o l'oscuramento di attività (come spegnere i transponder AIS delle navi). Le tecniche di inganno sono particolarmente efficaci quando rafforzano i pregiudizi o le aspettative preesistenti dell'analista. Ciò trasforma l'OSINT da una semplice ricerca della verità in una sorta di contesa controintuitiva, all'interno della quale l'analista deve non solo trovare informazioni accurate ma anche riconoscere e neutralizzare i tentativi attivi di inganno.

È quindi fondamentale un cambio di mentalità, che consenta di passare dal fact-checking passivo a una forma di consolidata consapevolezza delle proprie vulnerabilità cognitive.

PRIVACY, BIAS E USO RESPONSABILE

L'utilizzo dell'OSINT solleva questioni etiche complesse, in particolare riguardo alla **privacy**. Sebbene le informazioni siano pubblicamente disponibili, la loro aggregazione e analisi sistematica, specialmente da fonti come i social media, possono rivelare dettagli sensibili sulla vita privata, le opinioni, le relazioni o le abitudini di un individuo, che quella persona potrebbe non aver mai avuto l'intenzione di rendere così facilmente accessibili o collegabili. Il semplice fatto che un'informazione sia "pubblica" non ne giustifica automaticamente la raccolta o l'uso illimitato. È necessario rispettare le leggi sulla protezione dei dati (come il GDPR), ottenere il consenso quando possibile e appropriato, praticare la minimizzazione dei dati (raccogliere solo ciò che è strettamente necessario per l'obiettivo) e garantire trasparenza sui metodi utilizzati.

Il **bias (pregiudizio)** è un altro rischio significativo. Può manifestarsi a livello dell'analista, che potrebbe selezionare o interpretare le fonti in base a preconcetti personali, culturali, organizzativi, ecc...

Può però anche essere incorporato negli algoritmi di intelligenza artificiale utilizzati per l'analisi, portando a risultati distorti o discriminatori. Contrastare i bias richiede consapevolezza critica, diversità di prospettive nel team di analisi e validazione rigorosa dei risultati.

Infine, esiste il rischio intrinseco di **uso improprio (misuse)** dell'OSINT. Come già ricordato, le stesse tecniche utilizzate per scopi legittimi di sicurezza o investigazione possono essere impiegate da attori malintenzionati per stalking, molestie, frodi (come lo spear phishing personalizzato basato su informazioni raccolte online), pianificazione di attacchi fisici o informatici, o spionaggio aziendale. Questo sottolinea la necessità di quadri etici robusti, meccanismi di supervisione e responsabilità nell'uso dell'OSINT.

Le considerazioni etiche, in particolare sulla privacy, non sono solo questioni di conformità legale, ma sfide fondamentali per la legittimità e l'accettazione pubblica dell'OSINT. Man mano che le capacità OSINT diventano più potenti, specialmente con l'integrazione dell'IA, le possibilità di intrusione aumentano. Un fallimento nell'affrontare queste questioni etiche potrebbe portare a una reazione pubblica negativa pubblica e a normative più restrittive, limitando di fatto l'utilità stessa della disciplina.

COMPETENZE, STRUMENTI E LACUNE FORMATIVE

Condurre un'attività OSINT efficace non è banale e richiede risorse significative. Sono necessarie competenze analitiche specializzate, che includono pensiero critico, capacità di sintesi, conoscenza del dominio specifico, comprensione delle tecniche di verifica e consapevolezza dei bias. Sono spesso richieste anche competenze tecniche per utilizzare strumenti software avanzati, comprendere le infrastrutture di rete, analizzare metadati o navigare nel dark web.

L'accesso a **strumenti OSINT sofisticati** per la raccolta, l'elaborazione, l'analisi e la visualizzazione può essere un ostacolo. Ad esempio, molti strumenti richiedono abbonamenti costosi o licenze e ciò può creare un divario tra organizzazioni ben finanziate (agenzie governative, grandi aziende) e attori con risorse limitate (piccole ONG, giornalisti indipendenti, accademici).

Inoltre, l'ambiente OSINT è in **continua e rapida evoluzione**: nuove fonti emergono costantemente, piattaforme social cambiano le loro API o politiche sulla privacy, nuovi strumenti vengono sviluppati e le tecniche di inganno diventano più sofisticate.

Numero 5
giugno 2025

Mantenere aggiornate le proprie competenze e conoscenze richiede un impegno costante e risorse per la formazione continua. La mancanza di standardizzazione nelle metodologie e nella formazione può anche portare a variazioni nella qualità e nell'affidabilità dell'Intelligence prodotta. Questo divario di competenze e risorse rischia di portare a una concentrazione delle capacità OSINT più avanzate nelle mani di pochi attori potenti, statali o aziendali. Ciò potrebbe minare la potenziale "democratizzazione" spesso attribuito all'OSINT creando, anziché ridurla, un’asimmetria nel potere informativo.

IL FUTURO DELL'OSINT

L'OSINT è una disciplina in costante evoluzione, plasmata dai rapidi cambiamenti tecnologici e dall'adattamento delle pratiche di Intelligence. Diverse tendenze chiave stanno definendo il suo futuro, in particolare l'integrazione dell'intelligenza artificiale e le sinergie con altre forme di Intelligence.

INTEGRAZIONE DELL'INTELLIGENZA ARTIFICIALE (IA) E DEL MACHINE LEARNING (ML): OPPORTUNITÀ E RISCHI

L'impatto dell'Intelligenza Artificiale (IA) e del Machine Learning (ML) sull'OSINT è profondo e trasformativo. Queste tecnologie offrono opportunità significative per potenziare le capacità OSINT, ma introducono anche nuovi rischi e sfide.

Opportunità

- **Automazione della Raccolta e dell'Elaborazione:** L'IA può automatizzare compiti ripetitivi e dispendiosi in termini di tempo come il *web scraping*, il monitoraggio continuo dei social media e delle fonti di notizie e l'aggregazione di dati da fonti disparate. Ciò aiuta a gestire anche enormi volumi di dati.
- **Analisi avanzata:** Algoritmi di IA/ML possono analizzare grandi volumi di dati

Numero 5
giugno 2025

non strutturati (testo, immagini, video, audio) per identificare pattern nascosti, tendenze, anomalie e correlazioni che potrebbero sfuggire all'analisi umana. Tecniche come l'Elaborazione del Linguaggio Naturale (NLP) permettono l'analisi del sentiment, l'estrazione di entità (persone, luoghi, organizzazioni), la modellazione di argomenti e la traduzione multilingue. *La Computer Vision* consente il riconoscimento facciale, l'identificazione di oggetti e l'analisi di scene in immagini e video.

- **Analisi predittiva:** Analizzando dati storici e tendenze attuali, i modelli AI/ML possono contribuire a prevedere eventi futuri, identificare minacce emergenti o anticipare cambiamenti geopolitici, aggiungendo una dimensione proattiva all'OSINT.
- **Visualizzazione migliorata**: L'IA può facilitare la creazione di visualizzazioni complesse (mappe di rete, heatmap, mappe geospaziali) che aiutano gli analisti a comprendere relazioni complesse nei dati e a comunicare i risultati in modo efficace.
- **Fact-Checking e rilevamento della Disinformazione**: L'IA può assistere nella verifica dei fatti, nella valutazione della credibilità delle fonti e nel rilevamento automatico di contenuti manipolati come i deepfake.

Numero 5
giugno 2025

Rischi

- **Privacy:** L'automazione della raccolta dati su larga scala tramite IA può esacerbare le preoccupazioni relative alla privacy, raccogliendo potenzialmente grandi quantità di informazioni personali senza un adeguato controllo o consenso.

- **Bias algoritmici:** I modelli AI/ML possono ereditare o amplificare i bias presenti nei dati su cui sono addestrati, portando a risultati ingiusti, discriminatori o semplicemente errati. La mancanza di trasparenza ("*black box problem*") in alcuni algoritmi complessi può rendere difficile identificare e correggere questi bias.

- **Attacchi avversari**: Gli algoritmi di IA possono essere vulnerabili ad attacchi avversari, in cui input malevoli vengono creati appositamente per ingannare il modello e fargli produrre risultati errati.

- **"Allucinazioni" dell'IA**: I modelli generativi di IA possono talvolta produrre informazioni plausibili, ma completamente fabbricate ("allucinazioni"), che potrebbero essere scambiate per Intelligence valida se non verificate attentamente.

- **Dilemmi etici e supervisione:** L'uso di sistemi IA autonomi per la raccolta e l'analisi di Intelligence solleva questioni etiche complesse riguardo alla responsabilità, al controllo umano e al potenziale di abuso. Richiede quindi lo sviluppo di nuove competenze per gestire e supervisionare questi sistemi.

L'integrazione dell'IA nell'OSINT sta guidando una crescita significativa del mercato OSINT globale, con proiezioni economiche che ne indicano un'espansione sostanziale nei prossimi anni.

Tuttavia, l'efficacia futura dipenderà molto dalla capacità di bilanciare le notevoli potenzialità dell'IA con una gestione attenta dei rischi associati, in particolare per quanto riguarda l'etica, la privacy e l'affidabilità. L'emergere del "*black box problem*" sfida direttamente uno dei vantaggi principali dell'OSINT: la sua verificabilità. Se le conclusioni derivano da processi algoritmici opachi, diventa difficile per altri validare i risultati e ciò potrebbe potenzialmente minare la fiducia nell'Intelligence prodotta.

SINERGIE CON LE ALTRE INT IN EVOLUZIONE

Il futuro dell'OSINT sarà caratterizzato da una integrazione sempre più stretta con altre discipline di Intelligence, i cui confini stanno diventando più fluidi a causa della crescente disponibilità di dati precedentemente classificati o difficilmente accessibili.

GEOINT (Geospatial Intelligence): L'accesso a immagini satellitari commerciali ad alta risoluzione e a piattaforme di analisi geospaziale basate su cloud (come Google Earth Engine ha reso la GEOINT una componente fondamentale dell'OSINT. L'IA è essenziale per analizzare l'enorme volume di dati GEOINT generati dai crescenti asset satellitari commerciali e governativi.

È importante distinguere tra il dato GEOINT grezzo (l'immagine o l'informazione geospaziale) e l'analisi OSINT applicata a quel dato per produrre Intelligence.

Questa sinergia permette analisi dettagliate di movimenti militari, danni infrastrutturali, attività economiche e cambiamenti ambientali.

SOCMINT (Social Media Intelligence): I social media rimangono una fonte primaria per l'OSINT, fornendo insight su opinione pubblica, eventi in tempo reale, reti sociali e campagne di influenza.

L'IA sta rivoluzionando la SOCMINT, permettendo analisi su larga scala di testi, immagini e video, rilevamento di bot e analisi del sentiment con maggiore velocità e profondità.

Integrazione con INT Classificate: La relazione simbiotica tra OSINT e discipline classificate continuerà ad essere cruciale. L'OSINT fornirà sempre più spesso il quadro contestuale e gli spunti iniziali, mentre le INT classificate si concentreranno su lacune informative specifiche e sulla validazione di alto livello. L'obiettivo dovrà essere una fusione efficace di tutte le fonti ("*all-source fusion*") per ottenere il quadro informativo più completo possibile.

Altre fonti emergenti: L'OSINT si adatterà per sfruttare nuove fonti di dati aperti man mano che emergono, come dati da sensori IoT (*Internet of Things*), dati biometrici disponibili pubblicamente, o analisi di grandi dataset trapelati (leaked data).

Numero 5
giugno 2025

ISTITUZIONALIZZAZIONE E MAINSTREAMING NELLE COMUNITÀ DI INTELLIGENCE

Si osserva una chiara tendenza verso una maggiore formalizzazione e istituzionalizzazione dell'OSINT all'interno delle Agenzie di Intelligence e delle strutture di sicurezza nazionale a livello globale. Strategie nazionali dedicate (come quella dell'ODNI statunitense), la creazione di unità OSINT specifiche e progetti di sviluppo di capacità (come quelli della NATO) testimoniano questo riconoscimento formale.

Ciò si traduce in **maggiori investimenti** in strumenti software OSINT avanzati, piattaforme integrate, formazione del personale e reclutamento di analisti con competenze specifiche. Si sta lavorando anche allo sviluppo di standard professionali, dottrine e metodologie comuni per migliorare la qualità e la coerenza dell'Intelligence OSINT prodotta.

Numero 5
giugno 2025

La percezione dell'OSINT sta evolvendo da disciplina secondaria a componente fondamentale del ciclo di Intelligence, spesso considerata il punto di partenza ("first resort") per molte analisi. Tuttavia, come già a più riprese evidenziato, questa crescente integrazione solleva anche questioni importanti riguardo alla governance, all'etica e ai confini legali dell'uso statale dell'OSINT. Il dibattito su come bilanciare le esigenze di sicurezza nazionale con i diritti alla privacy e alla libertà di espressione nell'era digitale è in corso e plasmerà il futuro quadro normativo dell'OSINT.

Il futuro dell'OSINT sembra quindi orientato verso un **paradigma di collaborazione uomo-macchina (*human-machine teaming*)**. L'IA gestirà l'enorme scala dell'elaborazione dei dati, l'identificazione di pattern e l'automazione dei compiti ripetitivi, mentre gli analisti umani si concentreranno sugli aspetti che richiedono giudizio critico, comprensione contestuale profonda, verifica complessa, supervisione etica e interpretazione di situazioni ambigue o culturalmente sfumate. L'IA non sostituirà l'analista, ma ne aumenterà le capacità, spostando il ruolo umano verso funzioni cognitive di livello superiore.

TABELLA 2: MATRICE DELLE APPLICAZIONI OSINT IN GEOPOLITICA E CONFLITTI

Nota: Questa matrice illustra le connessioni principali. Molte applicazioni richiedono l'integrazione di più fonti e tecniche.

Area di applicazione	Fonti OSINT Primarie	Tecniche/Strumenti Chiave	Esempi/Riferimenti
Monitoraggio militare	Immagini Satellitari (Comm.), Social Media (UGC), Notizie Locali, Dati Trasporti	Geolocalizzazione, Cronolocalizzazione, Analisi Immagini (GEOINT), Monitoraggio Social Media, Analisi Metadati, Tracciamento Veicoli/Navi (AIS)	Build-up Russia-Ucraina , Perdite Equipaggiamento (Oryx) , Attraversamento Fiume , Identificazione Buk MH17, Ospedali da Campo
Analisi Disinformazione/Propaganda	Social Media, Notizie Online, Siti Web/Blog, Forum, Comunicazioni Ufficiali	Analisi Reti Sociali, Rilevamento Bot, Analisi Sentiment, NLP, Fact-Checking, Analisi Narrativa, Monitoraggio Media, Reverse Image Search, Deepfake Detection	Campagne Russe (Ucraina), Contesto MH17, Siria, Gray Zone Warfare, Inganno Strategico
Documentazione Crimini di Guerra	Social Media (UGC), Immagini Satellitari, Notizie Locali, Report ONG, Archivi Digitali	Geolocalizzazione, Cronolocalizzazione, Analisi Immagini/Video, Analisi Metadati, Riconoscimento Facciale, Archiviazione Sicura, Verifica Fonti	Siria (Armi Chimiche), Ucraina (Bucha, Esecuzioni, Deportazioni, Saccheggio Grano), Etiopia, Metodologie Bellingcat/GLAN
Analisi tendenze economiche	Notizie Finanziarie, Report Aziendali, Database Commerciali, Social Media, Dati Governativi	Analisi Sentiment (Mercato), Monitoraggio Prezzi/Valute, Analisi Report Finanziari, Web Scraping (Dati Economici)	Valutazione Salute Economica, Monitoraggio Mercati, Geopolitica Energia
Analisi sentimento pubblico	Social Media, Blog, Forum, Sondaggi Pubblici, Notizie	Analisi Sentiment (NLP), Monitoraggio Social Media, Analisi Trend Hashtag/Keyword, Analisi Reti di Discussione	Misurazione Opinione Pubblica, Reazioni a Eventi, Supporto Politiche 23, Monitoraggio Proteste
Monitoraggio sanzioni/commercio	Dati Tracciamento Navi (AIS), Registri Societari, Immagini Satellitari, Dati Doganali, Notizie	Tracciamento Marittimo (es. MarineTraffic), Analisi Corporate Records, Analisi Immagini Portuali, Analisi Dati Commerciali (es. Trade Map), Web Scraping	Evasione Sanzioni Iran 19, Analisi Flussi Commerciali 23, Monitoraggio Catene Approvvigionamento 14
Analisi intenzioni strategiche Stato	Comunicazioni Ufficiali, Report Governativi, Notizie, Pubblicazioni Accademiche, Dati Militari OSINT	Analisi Discorso, Monitoraggio Politiche, Analisi Budget Difesa, Monitoraggio Attività Diplomatiche, Analisi Dottrina Militare (da fonti aperte)	Analisi Politica Estera, Monitoraggio Piani Diplomatici, Inferire Intento Strategico

RACCOMANDAZIONI

SINTESI DELL'UTILITÀ DELL'OSINT NELLA GEOPOLITICA E NEI CONFLITTI

La panoramica presentata in questo lavoro conferma inequivocabilmente il ruolo indispensabile e crescente dell'Open Source Intelligence (OSINT) nel panorama della sicurezza e delle relazioni internazionali contemporanee. L'OSINT si è evoluta da una pratica marginale a una disciplina di Intelligence fondamentale, spesso definita "di prima istanza", capace di fornire indicazioni tempestive, accessibili e frequentemente verificabili su una vasta gamma di questioni geopolitiche e dinamiche conflittuali. La sua utilità si manifesta su più livelli:

- **Nella Geopolitica**, l'OSINT permette di monitorare le azioni e le intenzioni degli Stati (inclusi movimenti militari e posture strategiche), analizzare tendenze economiche globali (flussi commerciali, sanzioni, stabilità economica), valutare l'opinione pubblica e le campagne di influenza3 e comprendere le sfumature culturali e sociali, fornendo così un contesto cruciale per la diplomazia e la formulazione di politiche strategiche.
- **Nell'analisi dei conflitti**, l'OSINT offre una visibilità senza precedenti sul campo di battaglia (movimenti di truppe, danni, tattiche), funge da strumento essenziale

per la verifica dei fatti e il contrasto alla disinformazione in ambienti informativi degradati e gioca un ruolo sempre più vitale nella documentazione di potenziali crimini di guerra e violazioni dei diritti umani, supportando gli sforzi di accountability.

L'OSINT non opera in isolamento, ma in **sinergia con le discipline di Intelligence tradizionali**, fornendo spesso la conoscenza di base che permette alle risorse classificate di concentrarsi su obiettivi specifici e di alto valore. La sua natura aperta facilita inoltre la condivisione dell'Intelligence e la collaborazione internazionale.

AFFRONTARE LE SFIDE: VERSO BEST PRACTICE E QUADRI ETICI

Nonostante la sua indubbia utilità, l'efficacia e la legittimità dell'OSINT dipendono dalla capacità di affrontare le sue sfide intrinseche. Il sovraccarico informativo richiede strumenti e metodologie avanzate per filtrare e analizzare efficacemente l'enorme volume di dati disponibili.
La **questione della verifica** è fondamentale, data la prevalenza di misinformazione, disinformazione e tentativi deliberati di inganno nell'ambiente open source. Sono quindi necessarie metodologie rigorose di validazione e un approccio analitico critico e consapevole dei propri bias.

Le **implicazioni etiche**, in particolare riguardo alla privacy individuale, richiedono la massima attenzione. L'aggregazione di dati pubblici può portare a intrusioni non intenzionali nella sfera privata, rendendo indispensabile l'adesione a principi etici solidi (consenso, minimizzazione, trasparenza) e il rispetto dei quadri normativi esistenti. È prioritario sviluppare e adottare **quadri etici specifici per l'OSINT**, come l'OSINT *Privacy Impact Framework* (OPIF), per guidare le pratiche responsabili.

Infine, il **divario di risorse e competenze** tra diversi attori deve essere colmato attraverso investimenti in formazione, sviluppo di standard professionali e promozione di strumenti open source accessibili. L'integrazione dell'**Intelligenza Artificiale**, pur offrendo enormi potenzialità per automatizzare e potenziare l'analisi, introduce ulteriori complessità legate a bias algoritmici, trasparenza e rischi etici che necessitano di una governance attenta.

Numero 5
giugno 2025

RACCOMANDAZIONI STRATEGICHE PER SFRUTTARE EFFICACEMENTE L'OSINT

Per massimizzare il valore dell'OSINT minimizzandone i rischi, suggerisco le seguenti raccomandazioni strategiche, differenziate per attore:

- **Per Governi e Agenzie di Intelligence**
  - **Investire in capacità integrate:** Sviluppare capacità OSINT olistiche che integrino personale qualificato, processi definiti e strumenti tecnologici avanzati (inclusa l'IA), favorendo la sinergia con le discipline classificate.
  - **Promuovere la collaborazione uomo-macchina:** Adottare un approccio di ***human-machine teaming***, dove l'IA supporta l'analisi su larga scala e l'identificazione di pattern, mentre gli analisti umani si concentrano su giudizio critico, contesto, verifica e supervisione etica.
  - **Rafforzare verifica e contro-Disinformazione**: Sviluppare e implementare protocolli robusti per la verifica delle fonti aperte e capacità dedicate per identificare e contrastare attivamente la disinformazione e le operazioni di inganno.
  - **Stabilire standard etici e supervisione:** Adottare e far rispettare quadri etici e legali chiari per la raccolta e l'uso dell'OSINT, garantendo la protezione

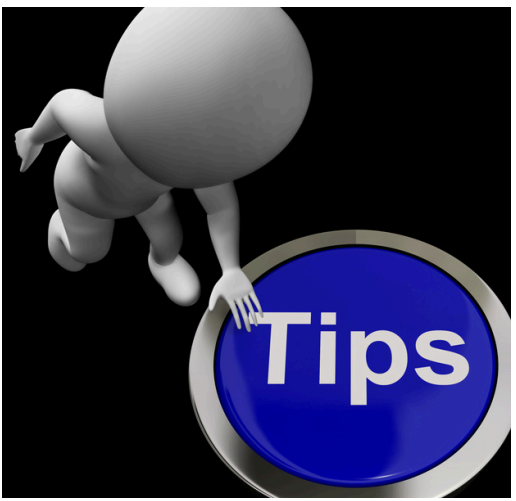
della privacy e meccanismi di supervisione efficaci.
    - **Facilitare la condivisione:** Sfruttare la natura aperta dell'OSINT per migliorare la condivisione di Intelligence all'interno del governo e con partner internazionali fidati.
    - **Prioritizzare formazione e competenze:** Investire nella formazione continua degli analisti per sviluppare competenze tecniche, analitiche e critiche necessarie per navigare l'ambiente OSINT complesso ed evolutivo.

- **Per Attori non Statali (Giornalisti, ONG, Ricercatori, Aziende):**
    - **Adottare metodologie rigorose:** Sviluppare e aderire a metodologie trasparenti e rigorose per la raccolta, la verifica (es. geolocalizzazione, cronolocalizzazione) e l'analisi OSINT, rispettando standard etici elevati, specialmente per la documentazione di abusi.
    - **Sfruttare la collaborazione**: Utilizzare piattaforme collaborative e reti di crowdsourcing per condividere risorse, verificare informazioni e amplificare l'impatto delle indagini.

- **Investire in formazione**: Cercare opportunità di formazione per acquisire competenze nell'uso di strumenti OSINT avanzati e nelle tecniche di analisi critica.
- **Trasparenza e limitazioni**: Essere trasparenti riguardo alle metodologie utilizzate e riconoscere apertamente le limitazioni delle proprie scoperte.
- **Advocacy**: Sostenere politiche che garantiscano l'accesso a dati pubblici e strumenti OSINT, promuovendo al contempo la protezione della privacy.

- **Per il mondo accademico:**
  - **Sostenere la ricerca:** Condurre ricerche su metodologie OSINT innovative, sull'integrazione responsabile dell'IA, sulle implicazioni etiche e legali, e sullo sviluppo di tecniche di verifica più robuste.
  - **Integrazione curriculare:** Incorporare moduli di formazione OSINT pratici ed etici nei curricula di discipline pertinenti come relazioni internazionali, giornalismo, studi sulla sicurezza, giurisprudenza e informatica.
  - **Promuovere la collaborazione:** Facilitare il dialogo e la collaborazione tra accademici, professionisti dell'Intelligence, giornalisti e *policy-maker* per condividere conoscenze e *best practice*.

- **Raccomandazioni generali**
  - **Promuovere l'alfabetizzazione digitale:** Educare il pubblico al pensiero critico e al consumo consapevole delle informazioni online per aumentare la resilienza collettiva alla disinformazione.
  - **Supportare strumenti Open Source:** Incoraggiare lo sviluppo e la diffusione di strumenti OSINT open source di alta qualità per ridurre il divario di risorse e promuovere l'accessibilità.
  - **Dialogo continuo sulla Governance:** Mantenere un dialogo aperto e inclusivo tra tutti gli stakeholder sull'evoluzione dell'OSINT, sulle sue implicazioni e sulla necessità di una governance adattiva ed efficace nell'era digitale.



LINK DI APPROFONDIMENTO

Protocollo di berkeley
https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source
OSINT: strumenti legali per aziende e investigatori privati
https://proteggimi.com/osint-decreto-231-investigazioni-private/
Osint e Regolamento DORA
https://proteggimi.com/osint-regolamento-dora-banche-compliance/
L'Osint nell'ambito della Direttiva Nis 2
https://proteggimi.com/osint-nis2-cybersecurity-pmi/
What is OSINT (Open-Source Intelligence?) - SANS Institute
https://www.sans.org/blog/what-is-open-source-Intelligence/
IC OSINT Strategy 2024-2026
https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf
What is Open -source Intelligence, and how is it used? - BreachLock
https://www.breachlock.com/resources/blog/what-is-open-source-Intelligence-and-how-is-it-used/
Ethical Frameworks in OSINT Final.pdf - Homeland Security
https://www.dhs.gov/sites/default/files/2022-09/Ethical%20Frameworks%20in%20OSINT%20Final.pdf

The Evolution of Open Source Intelligence (OSINT) From AFIO's THE IntelligenceR https://www.afio.com/publications/Schauer_Storger_Evo_of_OSINT_WINTERSPRING2013.pdf
Intelligence Studies: Open-Source Intelligence (OSINT) - LibGuides at Naval War College https://usnwc.libguides.com/c.php?g=494120&p=3420732
GEOINT Breaking Into OSINT Territory: The Future of Geospatial Technology in Warfare https://praescientanalytics.com/geoint-breaking-into-osint-territory-the-future-of-geospatial-technology-in-warfare/
Why OSINT Is the INT of First Resort - Booz Allen https://www.boozallen.com/insights/intel/why-osint-is-the-int-of-first-resort.html
Why OSINT Is the Cornerstone of Modern Intelligence - Babel Street https://www.babelstreet.com/blog/transforming-modern-Intelligence-with-open-source-Intelligence-osint
Open source Intelligence on the internet – categorisation and evaluation of search tools https://ejournals.eu/pliki_artykulu_czasopisma/pelny_tekst/0193de09-99a7-7153-b107-82520b9bd5d8/pobierz
A Brief History of Open Source Intelligence - bellingcat https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-Intelligence/

What is OSINT [Open-Source Intelligence]? Complete Guide - ShadowDragon.io
https://shadowdragon.io/blog/what-is-osint/
The Future of Open-Source Intelligence (OSINT): Market Growth, AI Integration, and Strategic Applications (2025-2034) - SpecialEurasia
https://www.specialeurasia.com/2025/03/24/osint-market-ai-integration/
OSINT in Gray Zone Warfare | Blog - Penlink
https://www.penlink.com/blog/osint-in-gray-zone-warfare/
NATO must recognize the potential of open-source Intelligence
https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-must-recognize-the-potential-of-open-source-Intelligence/
OSINT (Open Source Intelligence): uno strumento necessario per l'efficienza e la sicurezza del sistema aziendale
https://tesi.luiss.it/37848/1/257711_TRENTIN_GISELLA%20MARIA.pdf
Using OSINT in Geopolitical assessment: a practical guide - Authentic8,
https://www.authentic8.com/blog/osint-Geopolitical-assessment
The rise of open-source Intelligence | European Journal of international security
https://www.cambridge.org/core/journals/european-journal-of-international-security/article/rise-of-opensource-Intelligence/21122432399ECB8078BF0D89A76D0586

Open source Intelligence (OSINT) as an element of military recon https://securityanddefence.pl/Open-source-Intelligence-OSINT-as-an-element-of-military-recon,103337,0,2.html
How OSINT shaped reporting on the war in Ukraine - Centre for Information Resilience https://www.info-res.org/eyes-on-russia/articles/how-osint-shaped-reporting-on-the-war-in-ukraine/
Open Source Intelligence for War Crime Documentation - CEUR-WS.org https://ceur-ws.org/Vol-3654/short3.pdf
Open-Source Intelligence Is a Key Ingredient of Holistic SDA - Kratos Defense https://www.kratosdefense.com/constellations/articles/open-source-intelligence-is-a-key-ingredient-of-holistic-sda
OSINT (Open Source Intelligence) tra metodologia e funzione vitale per le aziende https://www.ictsecuritymagazine.com/articoli/osint-open-source-intelligence-tra-metodologia-e-funzione-vitale-per-le-aziende/
Malicious Life Podcast: Unmasking Secrets: The Rise of Open-Source Intelligence https://www.cybereason.com/blog/unmasking-secrets-the-rise-of-open-source-intelligence
Bellingcat: Courageous Journalism Unveiling the Truth Ahead of Britain https://www.newgeopolitics.org/2023/02/21/bellingcat-courageous-journalism-unveiling-the-truth-ahead-of-britain/

Discursive Warfare: Bellingcat Challenging Dominant Actors Liam Rydén - GUPEA https://gupea.ub.gu.se/bitstream/handle/2077/78411/Ryde%CC%81n.Liam.pdf?sequence=1&isAllowed=y
Open-source Intelligence: a valuable public tool for handling private disputes - S-RM https://www.s-rminform.com/latest-thinking/osint-in-dispute-resolution
OSINT Investigations: 9 Biggest Challenges - ShadowDragon.io https://shadowdragon.io/blog/what-are-the-common-struggles-of-osint-investigations/
OSINT Uncovered: Best Practices for Open-Source Intelligence - Osavul https://www.osavul.cloud/blog/osint-process-and-best-practices-for-open-source-Intelligence
Ethical issues of OSINT - UK Cyber Security Council https://www.ukcybersecuritycouncil.org.uk/blogs/blogs/ethical-issues-of-osint/
Open Source Investigation Best Practices 2025 - Neotas https://www.neotas.com/open-source-investigation-best-practices/
Preserving Privacy: An Impact Framework for Open-Source Intelligence (OSINT): Current State of Knowledge - New America https://www.newamerica.org/future-security/reports/preserving-privacy-an-impact-framework/current-state-of-knowledge/

The Emerging Role of AI in Open-Source Intelligence - The Hacker News https://thehackernews.com/2024/07/the-emerging-role-of-ai-in-open-source.html
What Are Open Source Investigations (OSINT)? - True People Check https://truepeoplecheck.com/osint-open-source-investigations/
What Is Open Source Intelligence (OSINT)? - SalesFuel https://salesfuel.com/what-is-open-source-Intelligence/
Integrating Earth observation IMINT with OSINT data to create added-value multisource Intelligence information: A case study of the Ukraine–Russia war - Security and Defence Quarterly https://securityanddefence.pl/Integrating-Earth-observation-IMINT-with-OSINT-data-to-create-added-value-multisource,170901,0,2.html
OSINT Techniques: Complete List for Investigators (2025) - ShadowDragon.io https://shadowdragon.io/blog/osint-techniques/
OSINT for Academic Literature · Jieyab89/OSINT-Cheat-sheet Wiki - GitHub https://github.com/Jieyab89/OSINT-Cheat-sheet/wiki/OSINT-for-Academic-Literature
Uncovering ground truth: Using GeoAI in OSINT & investigative journalism - Picterra https://picterra.ch/blog/uncovering-ground-truth-using-geoai-in-osint-investigative-journalism/

GEOINT Artificial Intelligence
https://www.nga.mil/news/GEOINT_Artificial_Intelligence_.html
Geospatial Intelligence (GEOINT) Basic Doctrine Publication 1-0
https://irp.fas.org/agency/nga/doctrine.pdf
GEOINT Lessons Being Learned from the Russian-Ukrainian War - USGIF
https://usgif.org/geoint-lessons-being-learned-from-the-russian-ukrainian-war/
AI in Open-Source Intelligence (OSINT) | How It Works, Benefits, and Challenges in Cybersecurity - Web Asha Technologies
https://www.webasha.com/blog/ai-in-open-source-Intelligence-osint-how-it-works-benefits-and-challenges-in-cybersecurity
AI-Powered OSINT Tools in 2025 | How Artificial Intelligence is Transforming Open-Source Intelligence Gathering - Web Asha Technologies
https://www.webasha.com/blog/ai-powered-osint-tools-in-2025-how-artificial-Intelligence-is-transforming-open-source-Intelligence-gathering
How can AI assist OSINT researchers | Barracuda Networks Blog
https://blog.barracuda.com/2025/02/18/ai-assist-osint-researchers
Dataset of Verified Videos About Chemical Weapons Attacks in Syria - Syrian Archive
https://syrianarchive.org/en/investigations/dataset-of-verified-videos-about-chemical-weapons-attacks-in-syria

Intelligence Preparation of the Battlefield - i2 Group
https://i2group.com/articles/geoint-and-i2
Russia's Invasion of Ukraine: A 12 Month Overview - ArcGIS StoryMaps
https://storymaps.arcgis.com/stories/0456b6687e4d47e0873a3398c6134554
A dataset of Open Source Intelligence (OSINT) Tweets about the Russo-Ukrainian war - arXiv https://arxiv.org/pdf/2409.01052
Full article: Intelligence & the Russo-Ukrainian war: introduction to the special issue
https://www.tandfonline.com/doi/full/10.1080/02684527.2024.2330132
Alessandro Accorsi: Disinformation Warfare in the Middle East - CSIS
ahttps://www.csis.org/analysis/alessandro-accorsi-disinformation-warfare-middle-east
Puzzling Pieces: OSINT and War Crime Accountability in Ukraine - RUSI
https://www.rusi.org/explore-our-research/publications/commentary/puzzling-pieces-osint-and-war-crime-accountability-ukraine
(PDF) Ukraine War OSINT Analysis: A Collaborative Student Report - ResearchGate
https://www.researchgate.net/publication/370500100_Ukraine_War_OSINT_Analysis_A_Collaborative_Student_Report

Open Source Intelligence: challenges and opportunities https://fjIntelligence.com/open-source-Intelligence/
Navigating the Maze of False Information during OSINT Investigations - Skopenow https://www.skopenow.com/news/navigating-false-information-during-osint
How open source evidence took a lead role in the response to the Douma chemical weapons attack - Amnesty International https://www.amnesty.org/en/latest/news/2018/04/how-open-source-evidence-took-a-lead-role-in-the-response-to-the-douma-chemical-weapons-attack/
Russia/Ukraine - Coming of Age for OSINT? - The World of Intelligence - Janes, https://podcast.janes.com/public/68/The-World-of-Intelligence-50487d09/0fd51eaa
The Transparency Trap: Risks of Deception in the Age of OSINT - U.S. Naval Institute https://www.usni.org/magazines/proceedings/2025/january/transparency-trap-risks-deception-age-osint
NATO Open Source Intelligence (OSINT) Capability https://www.act.nato.int/wp-content/uploads/2023/05/rfi022059_qa1a.pdf
Requirements Assessment - NATO's ACT https://www.act.nato.int/wp-content/uploads/2023/05/rfi022059_survey.xlsx

Open-source Intelligence: a comprehensive review of the current state, applications and future perspectives in cyber security https://pmc.ncbi.nlm.nih.gov/articles/PMC10014398/

Fundamentals of Open-Source Intelligence for Journalists | ICFJ https://www.icfj.org/news/fundamentals-open-source-Intelligence-journalists

MH17 The Open Source Evidence - Bellingcat https://www.bellingcat.com/app/uploads/2015/10/MH17-The-Open-Source-Evidence-EN.pdf

Using OSINT to track international weapons sales to conflict areas - Leone Hadavi https://www.youtube.com/watch?v=K-RHegh6Vlc

Integrating OSINT into Justice Processes | Institute for War and Peace Reporting, https://iwpr.net/global-voices/integrating-osint-justice-processes

Ukraine conflict: How can open-source Intelligence help prove war crimes? - Context News https://www.context.news/ai/how-can-open-source-Intelligence-help-prove-war-crimes

bellingcat - the home of online investigations https://www.bellingcat.com/

Seventh Report of the Organisation for the Prohibition of Chemical Weapons-United Nations Joint Investigative Mechanism - Security Council,

Nations Joint Investigative Mechanism - Security Council, https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2017_904.pdf
A/68/663–S/2013/735 General Assembly Security Council https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2013_735.pdf
OSINT - bellingcat https://www.bellingcat.com/tag/osint/
The future of online investigations with Bellingcat founder Eliot Higgins | Janes, https://podcast.janes.com/public/68/The-World-of-Intelligence-50487d09/fcc4bac3
(PDF) Open Source Intelligence Opportunities and Challenges: a Review - ResearchGate https://www.researchgate.net/publication/381074245_Open_Source_Intelligence_Opportunities_and_Challenges_a_Review
Geopolitical Intelligence Analysis for Strategic Insights https://www.insightforward.co.uk/blog/Geopolitical-Intelligence-analysis/
What Is OSINT in 2025: A Guide by Molfar https://molfar.com/en/blog/shcho-take-osint-u-2024-gaid-vid-molfar

Explaining and Developing the OSINT Privacy Impact Framework (OPIF) - New America
https://www.newamerica.org/future-security/reports/preserving-privacy-an-impact-framework/explaining-and-developing-the-osint-privacy-impact-framework-opif/
Future Trends in AI and Machine Learning for Cybersecurity - BitLyft
https://www.bitlyft.com/resources/future-trends-in-ai-and-machine-learning-for-cybersecurity
Open source Intelligence and AI: a systematic review of the GELSI literature - PMC
https://pmc.ncbi.nlm.nih.gov/articles/PMC9883130/