

Oltre il dato visibile: che cos'è oggi l'OSINT

Greta Furlan



International Institute for Global Analyses

Vision & Global Trends. International Institute for Global Analyses
Piazza dei Navigatori 22, 00147 – Rome (Italy)

The views and opinions expressed in this publication are those of the authors and do not represent the views of the Vision & Global Trends. International Institute for Global Analyses unless explicitly stated otherwise.

© 2026 Vision & Global Trends - International Institute for Global Analyses
© 2026 Greta Furlan

First Edition: September 2026

Analytical Dossier 17/2026 - ISSN 2704-6419

www.vision-gt.eu
info@vision-gt.eu

Oltre il dato visibile: che cos'è oggi l'OSINT

Greta Furlan



Vision & Global Trends – International Institute for Global Analyses

Oltre il dato visibile: che cos'è oggi l'OSINT

Greta Furlan

Beyond visible Data: What OSINT is today

Abstract - This paper examines the evolution and contemporary role of Open Source Intelligence (OSINT) in international security. It explores the transformation of publicly available information into verified intelligence through the systematic integration of geospatial data, social media, tracking systems, public records, and grey literature. Particular attention is devoted to the growing use of artificial intelligence, the continuing importance of human analytical judgment, and the risks posed by disinformation, spoofing, deepfakes, and cognitive biases. The study argues that OSINT has become an essential component of contemporary intelligence, while stressing the need for rigorous verification, contextual analysis, and methodological discipline.

Keywords: Open Source Intelligence (OSINT); Artificial Intelligence; International Security

1. Introduzione: La democratizzazione dell'intelligence

Nell'ambito della sicurezza internazionale moderna, l'OSINT, l'attività di intelligence basata sull'analisi metodica delle fonti aperte e accessibili al pubblico, costituisce uno strumento operativo consolidato per monitorare e comprendere gli scenari geopolitici globali.

Una dimostrazione lampante della portata di questa disciplina è avvenuta nel corso del 2021, quando, nel deserto cinese nei pressi di Yumen, sono stati individuati, da parte di Decker Eveleth del think tank CNS, 119 silos per missili nucleari ICBM (DF-41).¹

Gli analisti hanno scoperto i siti identificando grandi cupole gonfiabili, utilizzate per nascondere gli scavi, disposte in una griglia geometrica perfetta. Queste informazioni sono quindi riuscite ad invalidare la difesa di Pechino, che attribuiva quelle strutture alla realizzazione di un semplice parco eolico.

La principale novità risiede nel fatto che questa scoperta è avvenuta interamente utilizzando delle immagini satellitari commerciali della società privata Planet Labs.

Questo è soltanto uno dei numerosi eventi che dimostra come l'intelligence civile a fonti aperte (OSINT) possa anticipare, integrare o addirittura smentire le informative governative ufficiali.²

La sicurezza globale non è più un dominio ad accesso esclusivo delle agenzie statali; la diffusione degli strumenti OSINT ha trasformato il monitoraggio da un processo esclusivamente verticale ad uno orizzontale, in cui anche ricercatori indipendenti e giornalisti hanno la possibilità di svolgere indagini affidabili. Va inoltre sottolineato che questo cambiamento non elimina il perimetro del Segreto di Stato, in quanto le informazioni classificate restano sempre e comunque al di fuori del dominio delle fonti aperte.³

2. Il confine tra notizia e intelligence

Al fine di comprendere la reale portata di questa disciplina, è necessario sottolineare che l'Open Source Intelligence non coincide con la semplice reperibilità di informazioni sul web. L'espressione "fonti aperte" identifica un'accessibilità garantita per vie legali e pubbliche, segnando un netto distacco dai metodi clandestini di raccolta informativa.

¹ Warrick, J. (2021, July 1). China is building more than 100 new missile silos in its western desert, analysts say. The Washington Post

² Stein, L., & Armitage, R. (2021, July 9). China appears to be ramping up construction of missile silos in the desert. But could it be a 'shell game'? ABC News

³ European Union. (2022, May 2). What is OSINT: Open-source intelligence?. data.europa.eu.

Secondo il NATO Open Source Intelligence Handbook, l'OSINT comprende: «Informazioni individuate, selezionate, elaborate e diffuse a un pubblico specifico per rispondere a esigenze informative definite». ⁴Essa attinge a un'ampia varietà di canali pubblici: testate giornalistiche, comunicati istituzionali, letteratura grigia, atti parlamentari, registri societari, piattaforme social e pubblicazioni scientifiche.

Sul piano pratico, tuttavia, il valore operativo dipende dalla capacità di distinguere l'OSINT da quella che viene definita OSINF (Open Source Information). L'OSINF costituisce la materia prima grezza: l'insieme disordinato di dati accessibili al pubblico, privi di contestualizzazione, filtraggio o verifica. La transizione da informazione a intelligence avviene esclusivamente quando il dato viene processato, rielaborato e contestualizzato durante le varie fasi del ciclo operativo d'intelligence. Operare questa distinzione è indispensabile per quattro ragioni strategiche: elevare l'accuratezza e l'affidabilità del dato, ottimizzare l'allocazione delle risorse evitando la saturazione informativa, garantire la piena conformità ai vincoli etico-legali (dalla tutela dei dati personali alla catena di custodia) e snellire i processi decisionali. Un dato grezzo è intrinsecamente suscettibile di errori, manipolazioni e depistaggi; solo la trasformazione metodica consente di convertirlo in un dato OSINT verificato.⁵

3. Il mosaico delle fonti: canali e strumenti sul campo

Oggi la ricerca su fonti aperte non si limita più a raccogliere articoli di giornale: attualmente si configura come una struttura complessa e multidisciplinare, in cui i documenti scritti vanno ad integrarsi con sensori fisici, frequenze radio e immagini geospaziali.

Uno dei pilastri più innovativi è rappresentato dalla GEOINT su base aperta. Esistono infatti delle costellazioni civili e commerciali, come per esempio la rete europea Sentinel, equipaggiata con sensori di varia natura, come radar o immagini multispettrali, che consentono di monitorare i danni della guerra e le trasformazioni del terreno indipendentemente dal maltempo o dall'oscurità.

In aggiunta, la rete di satelliti Landsat, nata con scopi di ricerca scientifica e telecomunicazione, ha permesso di rilevare modifiche del territorio e tracciare movimenti di veicoli.

Specifici sensori termici a infrarossi vengono inoltre impiegati per tracciare in tempo reale incendi ed esplosioni nelle aree di conflitto precluse agli osservatori internazionali.⁶

Un secondo snodo fondamentale è costituito dal tracciamento della mobilità aerea e marittima. In ambito aeronautico, il perno operativo poggia sul protocollo ADS-B: i vettori trasmettono costantemente su frequenze radio non cifrate parametri essenziali, quali identificativo, altitudine, velocità e coordinate geografiche. Nascono di conseguenza piattaforme aperte, come FlightAware, Flightradar24 e ADS-B Exchange, che integrano i segnali captati da una rete globale e decentralizzata di ricevitori radio civili, permettendo agli analisti di monitorare ponti aerei logistici, missioni di ricognizione e rotte di aerei di Stato.⁷

Parallelamente, nel dominio marittimo l'obbligo internazionale dell'AIS (Automatic Identification System) consente di mappare il traffico mercantile su piattaforme come MarineTraffic e VesselFinder. Incrociando queste trasmissioni radio con i registri di bandiera, l'analista OSINT è in grado di identificare le anomalie di rotta, lo spegnimento volontario dei dispositivi di bordo e i trasferimenti illeciti di merci in mare aperto utilizzati per eludere i regimi di sanzioni o i controlli doganali.⁸

⁴ NATO. (2001). NATO open source intelligence handbook. Supreme Allied Commander Atlantic.

⁵OSINT Industries Team. (2025, November 18). OSINF vs OSINT: How data becomes open-source intelligence. OSINT Industries

⁶Dossier Difesa. (2025, 21 febbraio). Open Source Intelligence (OSINT).

⁷FlightAware. (s.d.). ADS-B: Automatic Dependent Surveillance-Broadcast.

⁸Nautical Almanac. (s.d.). AIS: Posizione e tracciamento delle navi.

Sul versante dell'interazione digitale si colloca la SOCMINT (Social Media Intelligence), incentrata sul tracciamento e sull'elaborazione dei flussi generati sulle piattaforme social e sui network di messaggistica istantanea. In contesti di crisi internazionale, canali Telegram, X e i feed video operano come veri e propri osservatori diffusi, offrendo testimonianze visive immediate, posizioni geografiche degli attacchi e dei movimenti di convogli militari. Tuttavia, la SOCMINT costituisce anche l'ambiente a più alto tasso di inquinamento, saturo di propaganda bellica, disinformazione orchestrata e alterazioni algoritmiche. Per l'analista, il rischio di convalidare operazioni di guerra psicologica (*psy-ops*) o incorrere in trappole cognitive è costante; ciò impone una rigorosa verifica dei metadati, la contestualizzazione cronologica e l'incrocio costante con evidenze fisiche.⁹

Accanto ai dati geospaziali, satellitari e di tracciamento, un ruolo determinante è svolto dalla letteratura grigia (*grey literature*) e dalla documentazione pubblica non convenzionale. Contrariamente a quanto si è soliti pensare, il termine "grigio" non allude a livelli intermedi di segretezza o a materiale parzialmente classificato, bensì alla vasta produzione documentale diffusa al di fuori dei circuiti editoriali commerciali e accademici convenzionali: rapporti tecnici preliminari, atti parlamentari, working paper, brevetti industriali, capitolati d'appalto e normative interne.

Per l'analista questa documentazione è fondamentale, perché rivela le reali intenzioni, le scelte strategiche e le mosse concrete degli attori coinvolti.

Unendo questi dati con registri pubblici e banche dati doganali, l'OSINT permette di ricostruire i flussi finanziari, seguire la pista di forniture militari o a duplice uso e smascherare le società di comodo usate per aggirare le sanzioni.

Senza il filtro di una redazione, però, serve sempre un'analisi critica per capire chi ha scritto il testo, con quali scopi e se ci si può fidare.¹⁰

E' però necessario sottolineare che nessuna di queste fonti, considerata singolarmente, offre certezze assolute: i segnali radio possono essere alterati, i riscontri social possono risultare manipolati e gli archivi documentali possono presentare lacune. Il vero valore dell'OSINT risiede dunque nella correlazione sistematica: è dalla convergenza tra tracciati di navigazione, evidenze satellitari e documentazione societaria che il dato grezzo si consolida in conoscenza analitica verificabile.

4. Intelligenza Artificiale e fattore umano nell'analisi contemporanea

Per comprendere la portata della rivoluzione tecnologica in atto, è utile ripercorrere l'evoluzione storica della disciplina. Le radici dell'OSINT moderna risalgono alla Seconda Guerra Mondiale, quando gli Alleati strutturarono il monitoraggio delle trasmissioni radiofoniche e della stampa nemica per decifrare le intenzioni dell'Asse. Durante la Guerra Fredda, questa prassi si consolidò: team di analisti e linguisti esaminavano quotidianamente le pubblicazioni ufficiali e le emissioni radiotelevisive del blocco sovietico alla ricerca di indizi operativi, agendo tuttavia in un contesto dominato dalla carenza informativa e dalla censura di regime.¹¹

La rivoluzione digitale e la diffusione della rete hanno capovolto radicalmente questo paradigma. Oggi l'analista non fronteggia più la scarsità del dato, bensì una massiccia ipertrofia informativa: una quantità enorme di contenuti generati ogni secondo, all'interno della quale la priorità diventa isolare gli aspetti rilevanti dal sovraccarico informativo.

Questo contesto ha favorito lo sviluppo dell'utilizzo dell'Intelligenza Artificiale per fronteggiare questa grande mole di dati. L'AI opera infatti come un moltiplicatore delle capacità umane: le

⁹ Istituto Investigativo Nacucchi. (2022, 12 dicembre). OSINT e SOCMINT: Cosa sono e come le usano gli investigatori.

¹⁰ Nacci, G. (s.d.). La letteratura grigia nella teoria generale dell'intelligence. LinkedIn Pulse.

¹¹ Dossier Difesa. (2025, 21 febbraio). Open Source Intelligence (OSINT).

tecniche di machine learning e deep learning permettono di elaborare rapidamente grandi volumi di dati operativi provenienti da sensori, piattaforme di intelligence, sorveglianza e ricognizione (*ISR*) e sistemi di comunicazione.

A ciò si accompagnano applicazioni di *computer vision*, grazie alle quali è possibile riconoscere oggetti in modo automatico, identificando sagome di mezzi militari, velivoli, armamenti o specifiche trasformazioni del terreno.¹²

Parallelamente, i modelli di elaborazione del linguaggio naturale (*NLP*) consentono di elaborare importanti testi, riconoscendo in modo preciso e rapido concetti chiave e traducendo in tempo reale idiomi rari, gerghi militari e canali di messaggistica locali.¹³

L'automazione non deve tuttavia marginalizzare il fattore umano.

I modelli di intelligenza artificiale presentano il rischio di incorporare o estendere distorsioni sistematiche (*bias*), capaci di alterare i risultati.

Essi possono infatti assorbire i pregiudizi della società presenti nei dati di addestramento, basarsi su convinzioni preesistenti (*bias di conferma*) o essere soggetti a manipolazioni mirate. Inoltre, il calcolo probabilistico dell'algoritmo non è in grado di cogliere le sfumature del contesto geopolitico e dell'inganno tattico. È quindi necessario che l'analista effettui un monitoraggio continuo, al fine di individuare e isolare quanto più possibile qualsiasi tipo di distorsione.¹⁴

Accanto all'evoluzione tecnologica e all'impiego dell'Intelligenza Artificiale, si assiste a una trasformazione ancora più radicale: la progressiva "democratizzazione" dell'intelligence e la conseguente perdita del monopolio informativo statale.

Se un tempo l'accesso ad analisi strategiche e osservazioni satellitari era un'esclusiva degli Stati, oggi la disponibilità di strumenti commerciali aperti a chiunque disponga di una connessione Internet ha ridotto drasticamente tale divario.

Questo scenario ha favorito l'emergere del giornalismo d'inchiesta partecipativo e di collettivi di ricerca, tra cui spicca Bellingcat, fondata nel 2014 da Eliot Higgins e descritta come una «agenzia di intelligence per il popolo».

Questa piattaforma è riuscita a dimostrare la grande solidità di questa metodologia grazie a diverse analisi effettuate tra cui quella sull'abbattimento del volo Malaysia Airlines 17 (MH17).

Incrociando semplici video amatoriali pubblicati dai residenti sui social con le mappe di Google Earth, i ricercatori sono riusciti a geolocalizzare e ricostruire l'intero tragitto del lanciamissili russo, documentandone il successivo rientro in territorio russo privo del missile impiegato nell'attacco.¹⁵

Questa apertura orizzontale porta con sé anche rischi concreti. Da una parte, diffondere informazioni sensibili in tempo reale può compromettere trattative riservate o canali diplomatici, che per funzionare richiedono discrezione. Dall'altra, gli apparati statali hanno imparato a strumentalizzare queste piattaforme a proprio vantaggio, facendo filtrare informazioni mirate a giornalisti e analisti indipendenti per promuovere narrative strategiche senza assumersi la piena responsabilità. Inoltre, l'assenza di filtri istituzionali e la corsa allo scoop aumentano il rischio di clamorosi errori di attribuzione. A ciò si aggiunge il problema della riservatezza: l'analisi massiva di foto e filmati sui social finisce spesso per esporre dati personali e mettere in pericolo cittadini comuni ripresi casualmente nei teatri di crisi.¹⁶

¹² Felisio, I. (2026, 23 marzo). Intelligenza artificiale militare: Applicazioni operative, architetture data-centriche e nuovi attori della defence-tech. Ce.S.I. - Centro Studi Internazionali.

¹³ IBM. (s.d.). Cos'è l'elaborazione del linguaggio naturale (NLP)? IBM Think Topics.

¹⁴ Holdsworth, J. (2023, 22 dicembre). Che cos'è il bias AI? IBM Think Topics.

¹⁵ Bellingcat Investigation Team. (2015, 8 ottobre). MH17: The open source evidence. Bellingcat

¹⁶ Damiano, L. (2021, 4 ottobre). OSINT, l'intelligence del popolo: vantaggi e rischi delle indagini a portata di clic. Agenda Digitale

5. *Le vulnerabilità del dominio aperto: manipolazione, inganno e bias cognitivi*

Se l'abbondanza di dati e l'accessibilità tecnologica offrono opportunità senza precedenti, esse espongono al contempo l'analista a un terreno operativo insidioso, dove l'evidenza aperta può trasformarsi nella più efficace delle armi d'inganno.

Un caso emblematico è rappresentato dal "finto avvicinamento" della HMS Defender alle coste della Crimea, orchestrato tramite la falsificazione dei dati di tracciamento marittimo (AIS) nel giugno 2021. In quell'occasione, le piattaforme pubbliche di monitoraggio navale mostravano il cacciatorpediniere britannico e una fregata olandese navigare ad alta velocità verso il porto di Sebastopoli, sede della flotta russa nel Mar Nero. In realtà, le due unità NATO non avevano mai lasciato gli ormeggi nel porto di Odessa, come documentato dalle webcam portuali trasmesse in diretta streaming. Ci si è trovati di fronte a una sofisticata operazione di spoofing: i segnali di posizionamento falsi sono stati generati da una stazione terrestre situata a Čornomors'k, con l'obiettivo di simulare un'incursione volontaria nelle acque contese, verificare la reazione difensiva delle forze russe e innescare una crisi politico-militare attraverso la manipolazione delle informazioni aperte.¹⁷

Un secondo fronte critico riguarda la disinformazione intenzionale e la proliferazione di contenuti sintetici, tra cui i *deep fake*. Nel marzo 2022, durante le prime settimane dell'invasione russa dell'Ucraina, è apparso in rete e sui canali compromessi dell'emittente ucraina Ukrayina 24 un video contraffatto in cui il presidente Volodymyr Zelensky invitava le proprie truppe a deporre le armi e ad arrendersi. La comunità OSINT ha smontato la manipolazione in pochi minuti: l'analisi tecnica ha evidenziato anomalie nell'intonazione vocale, una sproporzione tra testa e spalle, incoerenze nell'illuminazione del collo e difetti di sfocatura lungo il contorno delle labbra, tipici degli algoritmi di sintesi facciale.¹⁸

Accanto alle minacce tecnologiche, assume un peso determinante il fattore psicologico e cognitivo dell'operatore. L'analista è costantemente esposto al bias di conferma, ossia la tendenza a ricercare e valorizzare tra le fonti aperte solo quegli elementi che convalidano l'ipotesi di lavoro iniziale, scartando i segnali contrastanti. A questo si aggiunge il bias di disponibilità, che spinge a sopravvalutare un'informazione solo perchè è semplice da trovare, gratuita e accompagnata da immagini ad alta definizione, dimenticando tutto ciò che resta nascosto, o non rintracciabile sul web. Questa asimmetria genera una pericolosa «illusione di completezza»: l'errata convinzione che tutto ciò che si vede in rete costituisca l'intero quadro strategico, ignorando che le decisioni reali e le vere intenzioni degli attori passano quasi sempre lontano dai canali aperti.¹⁹

6. *Verso una nuova maturità metodologica: l'OSINT nell'era dell'iperconnessione*

L'OSINT è ormai un pilastro irrinunciabile dell'intelligence contemporanea. Quella che un tempo sembrava una curiosità per ricercatori della rete si è trasformata in una disciplina rigorosa, indispensabile per interpretare le crisi globali e guidare le scelte strategiche.

È fondamentale sottolineare come l'Open Source Intelligence non miri a sostituire le forme classiche di spionaggio, come le fonti umane (HUMINT) o l'intercettazione dei segnali (SIGINT). Al contrario, le due cose si integrano: il web offre una base trasparente e vastissima per inquadrare il problema, verificare le prime ipotesi e indirizzare in modo più efficiente le risorse investigative e le operazioni coperte.

¹⁷EUvsDisinfo. (2021, 24 giugno). British military ship Defender deliberately entered into Russian territorial waters in June 2021.

¹⁸Mastrolonardo, R. (2022, 17 marzo). Zelensky invita alla resa: il falso video creato dai russi con l'intelligenza artificiale. Sky TG24.

¹⁹Lapi, M. (s.d.). Il bias di conferma nell'OSINT: una guida pratica per analisti. Mirko Lapi Blog.

Certo, il dominio pubblico presenta molti rischi: operazioni di inganno, falsificazione dei segnali, *deepfake* e trappole mentali per gli analisti. Ma questi ostacoli non svalutano l'OSINT; anzi, ne rafforzano il metodo, imponendo verifiche incrociate sempre più rigorose e un approccio critico oggi fondamentale.

In un mondo sommerso da una marea di dati e algoritmi, il vero vantaggio competitivo non sarà di chi accumula più informazioni, ma dell'analista capace di unire i pezzi, capire il contesto geopolitico e separare la notizia utile dal rumore di fondo, senza mai dimenticare che la rete non mostrerà mai l'intero quadro della realtà.

Greta Furlan – Studentessa presso l'Università degli Studi Internazionali di Roma – Corso di laurea magistrale 'Investigazione, Criminalità e Sicurezza Internazionale'. Laurea triennale in Scienze Sociologiche. Presso l'Università degli Studi di Padova. Tirocinante presso Vision & Global Trends International Institute for Global Analyses, nell'ambito del progetto [Società Italiana di Geopolitica](#).

BIBLIOGRAFIA

Bellingcat Investigation Team. (2015, 8 ottobre). MH17: The open source evidence. Bellingcat. <https://www.bellingcat.com/news/europe/2015/10/08/mh17-the-open-source-evidence/>

Damiano, L. (2021, 4 ottobre). OSINT, l'intelligence del popolo: vantaggi e rischi delle indagini a portata di clic. Agenda Digitale. <https://www.agendadigitale.eu/sicurezza/osint-lintelligence-del-popolo-vantaggi-e-rischi-delle-indagini-a-portata-di-clic/>

Dossier Difesa. (2025, 21 febbraio). Open Source Intelligence (OSINT). <https://www.dossierdifesa.it/2025/02/21/open-source-intelligence-osint/>

European Union. (2022, May 2). What is OSINT: Open-source intelligence?.data.europa.eu. <https://data.europa.eu/en/publications/datastories/what-osint-open-source-intelligence>

EUvsDisinfo. (2021, 24 giugno). British military ship Defender deliberately entered into Russian territorial waters in June 2021. <https://euvsdisinfo.eu/it/report/british-military-ship-defender-deliberately-entered-into-russian-territorial-waters-in-june-2021/>

Felisio, I. (2026, 23 marzo). Intelligenza artificiale militare: Applicazioni operative, architetture data-centriche e nuovi attori della defence-tech. Ce.S.I. - Centro Studi Internazionali. <https://www.cesi-italia.org/it/articoli/intelligenza-artificiale-militare-applicazioni-operative-architetture-data-centriche-e-nuovi-attori-della-defence-tech>

FlightAware. (s.d.). ADS-B: Automatic Dependent Surveillance-Broadcast. <https://it.flightaware.com/adsb/>

Holdsworth, J. (2023, 22 dicembre). Che cos'è il bias AI? IBM Think Topics. <https://www.ibm.com/it-it/think/topics/ai-bias>

IBM. (s.d.). Cos'è l'elaborazione del linguaggio naturale (NLP)? IBM Think Topics.
<https://www.ibm.com/it-it/think/topics/natural-language-processing>

Istituto Investigativo Nacucchi. (2022, 12 dicembre). OSINT e SOCMINT: Cosa sono e come le usano gli investigatori.

<https://www.investigazioninacucchi.com/osint-e-socmint/>

Lapi, M. (s.d.). Il bias di conferma nell'OSINT: Una guida pratica per analisti. Mirko Lapi Blog.
<https://mirkolapi.com/blog/il-bias-di-conferma-nellosint-una-guida-pratica-per-analisti/>

Mastrolonardo, R. (2022, 17 marzo). Zelensky invita alla resa: il falso video creato dai russi con l'intelligenza artificiale. Sky TG24.

<https://tg24.sky.it/mondo/2022/03/17/zelensky-video-falso-deepfake-ucraina-russia>

Nacci, G. (s.d.). La letteratura grigia nella teoria generale dell'intelligence. LinkedIn Pulse.
<https://www.linkedin.com/pulse/la-letteratura-grigia-nella-teoria-generale-per-delle-giovanni-nacci/>

NATO. (2001). NATO open source intelligence handbook. Supreme Allied Commander Atlantic.
<https://ia801403.us.archive.org/32/items/NATOOSINTHandbookV1.2/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf>

Nautical Almanac. (s.d.). AIS: Posizione e tracciamento delle navi.
<https://www.nauticalalmanac.it/it/navigazione-marittima/ais-posizione-delle-navi>

OSINT Industries Team. (2025, November 18). OSINF vs OSINT: How data becomes open-source intelligence. OSINT Industries.

<https://www.osint.industries/post/osinf-vs-osint-difference-between-information-and-intelligence>

Stein, L., & Armitage, R. (2021, July 9). China appears to be ramping up construction of missile silos in the desert. But could it be a 'shell game'? ABC News.

<https://www.abc.net.au/news/2021-07-10/china-appears-to-be-ramping-up-construction-of-missile-silos/100273208>

Warrick, J. (2021, July 1). China is building more than 100 new missile silos in its western desert, analysts say. The Washington Post.

<https://www.missiledefenseadvocacy.org/threat-news/china-is-building-more-than-100-new-missile-silos-in-its-western-desert-analysts-say/>



Vision & Global Trends - International Institute for Global Analyses

www.vision-gt.eu

info@vision-gt.eu