Numero 8 - novembre 2025

OLTRE L'AULA DI TRIBUNALE: UN NUOVO STANDARD PER L'ANALISI OSINT

MIRKO LAPI

EXECUTIVE SUMMARY

Come già evidenziato nel whitepaper "L'Open Source Intelligence nella geopolitica e nell'analisi dei conflitti", l'Intelligence da fonti aperte (OSINT) è oggi pubblicamente riconosciuta come l'«INT di prima istanza» (INT of first resort), una disciplina primaria e fondamentale nel ciclo di Intelligence moderno, indispensabile per decifrare le complesse dinamiche dei conflitti e della politica internazionale. Tuttavia, al di là di questa fondamentale constatazione, si cela a mio avviso un potenziale ancora inesplorato, una possibilità di elevare la pratica dell'analisi OSINT a un nuovo livello di rigore e credibilità.

La tesi principale di questo nuovo approfondimento sostiene che i principi metodologici del Protocollo di Berkeley, ovvero un quadro metodologico concepito per garantire l'ammissibilità e la solidità delle prove digitali dinanzi alle più alte corti internazionali, possono rappresentare una struttura trasformativa di riferimento anche per l'analisi geopolitica.

In un'epoca sempre più caratterizzata dalla guerra dell'informazione, dalla disinformazione strategica e dall'inganno deliberato, ritengo che l'adattamento di questo quadro metodologico dal dominio legale a quello dell'Intelligence da fonti aperte, oltre che un'opportunità di miglioramento, rappresenta anche un'indubbia necessità strategica.

Questo lavoro segue un percorso concettuale ben definito. In primo luogo, si procederà a una decostruzione approfondita delle fondamenta giuridiche del Protocollo di Berkeley, esaminandone i principi cardine nel loro scopo originario. Successivamente, si analizzeranno criticamente le missioni divergenti dell'indagine giudiziaria e dell'analisi OSINT, con particolare attenzione alle distinte finalità che rendono inappropriata e concettualmente non corretta l'applicazione diretta del Protocollo. È in questo divario che risiede la necessità di un adattamento. Si propone quindi un nuovo quadro di riferimento che definisco come il "Protocollo per l'integrità analitica", il cui obiettivo è reinterpretare i principi del Protocollo di Berkeley per il mondo dell'Intelligence, un mondo che non deve ricercare la certezza retrospettiva del giudizio, bensì la valutazione probabilistica della previsione.

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.

Questo sforzo di adattamento è fondamentale perché, come si argomenterà, l'avversario principale nell'analisi geopolitica non è dato soltanto dall'inganno di un attore esterno, ma anche e soprattutto dai bias degli analisti, vulnerabilità che possono essere mitigate da un quadro metodologico rigoroso e specificamente progettato.

Per comprendere la portata e il potenziale di un adattamento del Protocollo di Berkeley, è prima di tutto indispensabile analizzarne in profondità la struttura e la finalità originarie. Il Protocollo non rappresenta una semplice lista di controllo, ma un sistema olistico e coerente, progettato per risolvere un problema specifico e di enorme portata: conferire a informazioni digitali, per loro natura volatili e facilmente manipolabili, la solidità e l'integrità necessarie per resistere al vaglio delle più alte giurisdizioni penali internazionali.

INDICE

ORIGINE E NATURA DEL PROTOCOLLO DI BERKELEY

Il Protocollo di Berkeley nasce da uno sforzo congiunto dell'Ufficio dell'Alto Commissario delle Nazioni Unite per i Diritti Umani (OHCHR) e del Human Rights Center della School of Law dell'Università della California, Berkeley. La sua creazione è stata una risposta diretta e necessaria alla crescente ondata di informazioni digitali provenienti da zone di conflitto e crisi umanitarie.

L'avvento degli smartphone e dei social media ha trasformato chiunque in un potenziale documentarista, generando un volume senza precedenti di contenuti generati dagli utenti (User-Generated Content - UGC) raffiguranti possibili violazioni dei diritti umani. Tuttavia, questo materiale veniva utilizzato in modo largamente "ad hoc", con organizzazioni e organismi investigativi che faticavano ad adattare le proprie prassi per gestire e convalidare queste nuove forme di prova. La necessità di "standard metodologici comuni sull'autenticazione e la verifica" era quindi diventata impellente per garantire che tali informazioni potessero essere considerate affidabili e, in ultima analisi, utilizzabili a fini di giustizia.

I principi cardine del protocollo

Prima di addentrarsi nell'analisi dettagliata dei principi cardine che costituiscono l'ossatura del Protocollo di Berkeley, è fondamentale riconoscere come questi rappresentino pilastri essenziali per la credibilità e la solidità delle prove digitali. Essi non solo garantiscono un approccio rigoroso nella gestione delle informazioni, ma offrono anche un riferimento etico e operativo indispensabile per chiunque operi nel campo dell'Intelligence da fonti aperte e nelle investigazioni digitali. L'elenco che segue intende illustrare, in modo chiaro e sistematico, le regole di base che permettono di trasformare dati digitali apparentemente fragili in elementi di prova robusti e affidabili, capaci di resistere alle sfide poste dalla giustizia e dalla complessità geopolitica contemporanea.

1) Il rigore metodologico

Il cuore del Protocollo risiede nella standardizzazione globale delle procedure per l'identificazione, la raccolta, la conservazione, la verifica e l'analisi delle informazioni digitali open source.

L'obiettivo è stabilire con il più alto grado di certezza possibile che un dato contenuto digitale (una foto, un video) sia ciò che afferma di essere, rappresentando un evento reale accaduto in un luogo e in un tempo specifici.

Per raggiungere questo obiettivo, il Protocollo si fonda su tecniche di verifica pratiche e rigorose, che sono diventate il marchio di fabbrica delle moderne indagini open source. Tra queste, due sono di fondamentale rilevanza:

- geolocalizzazione: questa tecnica consiste nel determinare la posizione geografica esatta in cui una foto o un video sono stati registrati. L'analista identifica punti di riferimento visivi unici nell'immagine (edifici, montagne, minareti, linee elettriche) e li confronta con immagini satellitari (come quelle disponibili su Google Earth o Sentinel Hub), mappe (come OpenStreetMap) o altre fonti geospaziali per trovare una corrispondenza univoca.

Questo processo permette di confermare o smentire la presunta localizzazione di un evento;

- cronolocalizzazione: complementare alla geolocalizzazione, questa tecnica mira a determinare il momento in cui un'immagine è stata catturata. Ciò può essere ottenuto attraverso vari metodi, come l'analisi delle ombre proiettate dagli oggetti. Conoscendo la posizione esatta (tramite geolocalizzazione) e la data, è possibile utilizzare strumenti come SunCalc per calcolare la posizione del sole in quel giorno e confrontarla con la lunghezza e la direzione delle ombre visibili nell'immagine, restringendo così la finestra temporale a poche ore o addirittura minuti. Altri metodi includono il confronto con immagini satellitari di date diverse per osservare cambiamenti nel terreno o la correlazione dell'evento con altre notizie o eventi noti accaduti in un determinato momento.

Queste tecniche, insieme all'analisi dei metadati (quando disponibili e non alterati) e alla ricerca inversa di immagini per trovare occorrenze precedenti del contenuto, costituiscono il fondamento metodologico per stabilire l'autenticità, un requisito non negoziabile nel contesto giudiziario.

2) La preservazione della catena di custodia

Nel diritto, non è sufficiente che una prova sia autentica; è necessario dimostrare che la sua integrità è stata preservata in ogni momento, dalla raccolta alla presentazione in tribunale. Il Protocollo di Berkeley sottolinea che, affinché un'informazione sia ammissibile come prova, l'accusa deve essere in grado di stabilirne l'autenticità e la catena di custodia (chain of custody).

Questo principio richiede una documentazione meticolosa e ininterrotta che tracci ogni passaggio del "viaggio" della prova digitale. L'investigatore deve registrare come l'informazione è stata scoperta, come è stata acquisita (ad esempio, scaricata da una piattaforma social), dove e come è stata archiviata e chi vi ha avuto accesso. Ogni azione deve essere documentata per dimostrare che il file originale non è stato alterato, manomesso o contaminato. L'uso di *hash* crittografici (impronte digitali uniche per ogni file) è una pratica standard per verificare che una copia di un file sia identica all'originale. Questo rigore è assoluto, poiché metodi di raccolta e conservazione non validi rendono l'informazione inaffidabile e quindi inutilizzabile ai fini di un processo legale.

3) Imperativi etici e di sicurezza

Il Protocollo è saldamente ancorato al diritto internazionale dei diritti umani e pone un'enfasi assoluta sulla protezione degli individui coinvolti nel processo investigativo.

Riconosce che la documentazione di gravi crimini può mettere a rischio la vita e il benessere di chi la produce e di chi la raccoglie. Pertanto, il Protocollo delinea misure per garantire la "sicurezza digitale, fisica e psicosociale" degli investigatori, dei testimoni, delle vittime e dei primi soccorritori (cittadini, attivisti, giornalisti).

Inoltre, il Protocollo affronta la complessa questione della privacy. Sebbene le informazioni OSINT siano, per definizione, pubblicamente disponibili, la loro aggregazione, analisi e conservazione sistematica possono costituire una significativa intrusione nella vita privata di un individuo. Il Protocollo fornisce quindi una guida su come bilanciare la necessità di accertare i fatti con il diritto fondamentale alla privacy, raccomandando pratiche come la minimizzazione dei dati (raccogliere solo ciò che è strettamente necessario) e l'anonimizzazione delle informazioni personali quando non sono pertinenti all'indagine.

La democratizzazione delle prove e le sue conseguenze strategiche

L'esistenza stessa del Protocollo di Berkeley non è solo un progresso metodologico, ma il segnale di un cambiamento di paradigma fondamentale nel panorama informativo globale. La sua creazione è la formalizzazione del fatto che attori non statali (giornalisti investigativi, organizzazioni non governative e persino singoli cittadini) sono diventati generatori primari di prove di rilevanza legale e strategica. Questa "democratizzazione delle prove" ha alterato irrevocabilmente l'ecologia dell'informazione nei conflitti.

Il processo logico che porta a questa conclusione è chiaro. In primo luogo, si è assistito all'ascesa di questi attori non statali e alla diffusione di capacità investigative precedentemente riservate agli Stati. In secondo luogo, il Protocollo di Berkeley è stato sviluppato proprio per standardizzare e professionalizzare il flusso di informazioni digitali provenienti da queste nuove fonti, con l'obiettivo esplicito di renderle utilizzabili per la giustizia. La conseguenza inevitabile è che gli attori statali non possono più esercitare un controllo monopolistico sulla narrazione delle loro azioni, specialmente in zone di conflitto. Sono ora soggetti al monitoraggio e al giudizio di una rete globale e decentralizzata di investigatori che operano secondo standard sempre più rigorosi e riconosciuti a livello internazionale.

Questo nuovo scenario, a sua volta, crea un potente incentivo per quegli stessi attori statali a intensificare e sofisticare le loro operazioni di guerra dell'informazione. Se l'ambiente open source è il nuovo terreno di scontro per la legittimità e la responsabilità, allora diventa strategicamente imperativo per un attore che compie azioni controverse tentare di "inquinare" o "intossicare" questo ambiente con disinformazione, dati manipolati e narrazioni fuorvianti.

Questo ciclo di azione e reazione rende l'adozione di un quadro metodologico rigoroso non solo prioritario per gli investigatori, ma assolutamente essenziale anche per qualsiasi analista, specialmente nel campo dell'Intelligence, che si affida alle fonti aperte per comprendere il mondo.

MISSIONI DIVERGENTI - GLI OBIETTIVI DELL'INDAGINE GIUDIZIARIA E DELL'ANALISI OSINT

Aver stabilito la solidità e lo scopo del Protocollo di Berkeley è il primo passo. Il secondo altrettanto importante, è riconoscere perché questo quadro, nella sua forma originale, non può essere semplicemente trasposto nel dominio dell'analisi OSINT. Applicare direttamente le stesse procedure rappresenterebbe un errore categoriale, cioè una confusione tra ambiti concettualmente distinti: in questo caso, si tratterebbe di sovrapporre senza distinzione il contesto investigativo e quello dell'analisi di Intelligence.

Le missioni fondamentali dell'investigatore, orientate alla raccolta di prove per un procedimento giudiziario, e quelle dell'analista di Intelligence, focalizzate invece sulla produzione di valutazioni strategiche per supportare decisioni in condizioni di incertezza, sono infatti intrinsecamente diverse sia negli obiettivi perseguiti, sia negli standard di prova adottati, sia nei prodotti finali che realizzano. Un errore categoriale si verifica proprio quando si applicano criteri o metodi di un ambito a un altro che risponde a logiche differenti: ad esempio, pretendere che l'analisi di Intelligence raggiunga la stessa certezza e rigore probatorio richiesti in sede giudiziaria significherebbe ignorare la natura probabilistica e interpretativa che caratterizza il lavoro dell'analista. Comprendere questa divergenza è il presupposto per qualsiasi tentativo di adattamento.

La ricerca della prova da parte dell'investigatore

Il contesto dell'investigazione legale, per cui è stato sviluppato il Protocollo di Berkeley, richiede l'accertamento rigoroso dei fatti relativi a eventi passati al fine di attribuire responsabilità giuridiche. Lo scopo non è speculare sulle cause, ma dimostrare con prove certe.

Obiettivo: l'investigatore cerca di costruire un caso che possa resistere al vaglio di un tribunale. L'obiettivo è l'accertamento della verità storica di un evento specifico. Ad esempio, non si tratta di valutare la probabilità che un missile abbia abbattuto un aereo, ma di provare, al di là di ogni

ragionevole dubbio, che un missile specifico, lanciato da un'unità militare specifica, in un dato momento e luogo, ha causato l'abbattimento di un velivolo.

Standard di prova: lo standard è elevato e spesso binario. Una prova è autentica o non lo è; una catena di custodia è integra o è interrotta; un imputato è colpevole o non colpevole. Non c'è spazio per l'ambiguità o la valutazione probabilistica tipica dell'Intelligence. L'informazione deve raggiungere una soglia di affidabilità tale da essere considerata un fatto accertato.

Prodotto finale: il risultato del lavoro dell'investigatore è un fascicolo probatorio, un insieme di prove digitali e documentali destinate a essere presentate a una corte, a un tribunale penale internazionale o a una commissione d'inchiesta. Il pubblico di questo prodotto sono giudici o giurie, il cui compito è emettere un verdetto definitivo.

La ricerca dell'intuizione da parte dell'analista

L'analista OSINT, al contrario, opera in un mondo di incertezza, incompletezza e inganno. La sua missione non è provare eventi passati, ma fornire ai decisori la migliore comprensione possibile di situazioni attuali e future per informare le loro scelte. Lo scopo dell'OSINT in questo contesto è "produrre conoscenza utile a supportare processi decisionali".

Obiettivo: l'analista si sforza di valutare probabilità, discernere le intenzioni di attori statali (e non) e prevedere eventi futuri. Il suo compito è ridurre l'incertezza per il decisore, non eliminarla. Ad esempio, di fronte a un massiccio dispiegamento militare, l'analista non deve "provare" che un'invasione avverrà, ma valutare la probabilità che si verifichi, considerare scenari alternativi (ad esempio, una mossa di diplomazia coercitiva) e identificare indicatori che potrebbero segnalare un cambiamento nelle intenzioni dell'avversario.

Standard della prova: questo standard presenta una natura dinamica ed è comunicato attraverso il livello di attendibilità e/o probabilità espresso. Le conclusioni sono raramente definitive, ma vengono qualificate mediante termini quali, ad esempio: "alta confidenza", "moderata confidenza" o "bassa confidenza". L'analisi privilegia la gestione dell'ambiguità e l'interpretazione delle sfumature, piuttosto che perseguire una visione dicotomica della verità.

Prodotto finale: l'output dell'analista è un report di Intelligence, un briefing o una valutazione destinata a un decisore politico, un comandante militare o uno stratega aziendale. Questo prodotto non è un verdetto, ma uno strumento per informare una decisione che deve essere presa in condizioni di informazione imperfetta.

La tensione tra certezza retrospettiva e ambiguità prospettica

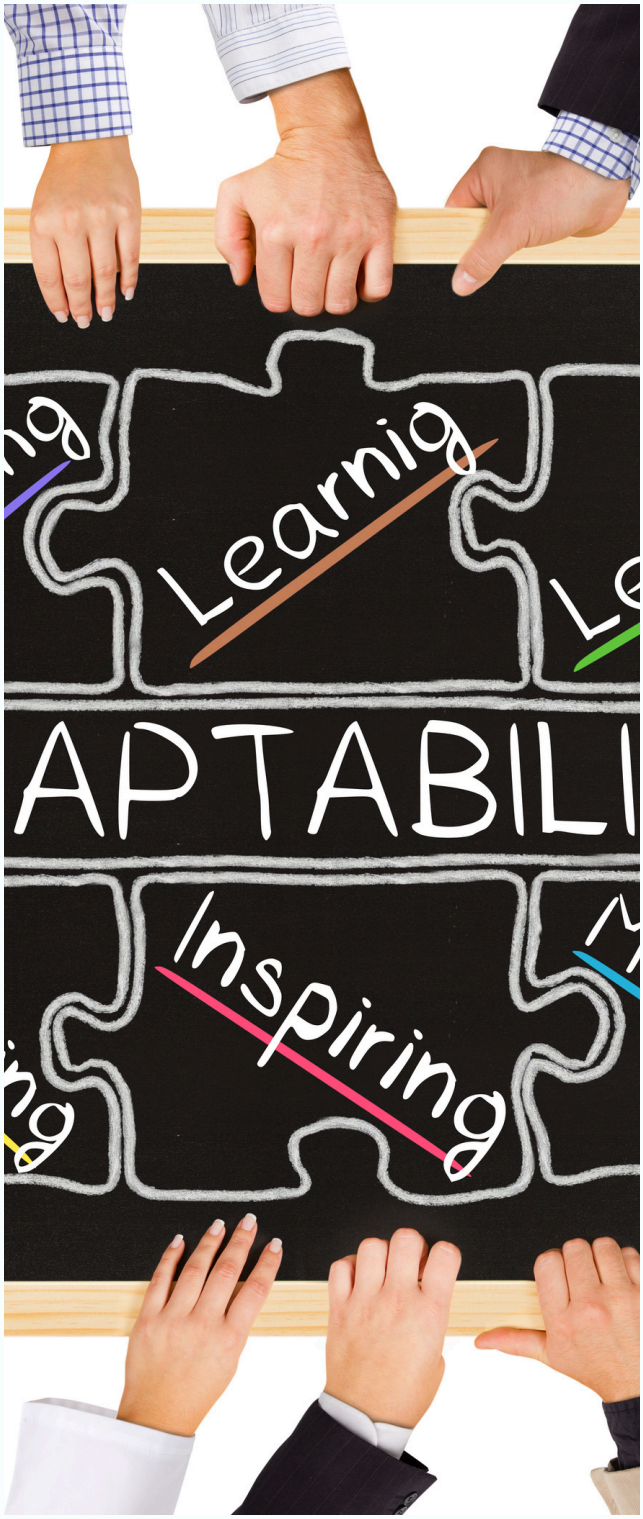
La distinzione fondamentale tra queste due discipline risiede nella loro direzione temporale e nei loro obiettivi epistemologici. L'indagine legale è intrinsecamente retrospettiva e persegue la certezza “oltre ogni ragionevole dubbio”. L'analisi Intelligence è prevalentemente prospettica e naviga nell'ambiguità intrinseca del futuro.

Questa tensione è il motivo per cui un'applicazione diretta del Protocollo di Berkeley all'analisi OSINT è impossibile e fuorviante.

Il linguaggio e i concetti del Protocollo sono radicati nella logica della prova. Si parla di "stabilire fatti" e di "ammissibilità in tribunale". L'Intelligence, d'altra parte, si occupa di comprendere "intenzioni strategiche", "tendenze geopolitiche", ecc...

Questi sono concetti che non possono essere "provati" nello stesso modo in cui si prova la traiettoria di un proiettile. Non si può, ad esempio, stabilire la "catena di custodia" di un'intenzione futura o "l'autenticità" di una tendenza emergente.

Pertanto, l'adattamento del Protocollo richiede una traduzione concettuale fondamentale. I suoi principi devono essere trasposti da un linguaggio di prova a un linguaggio di confidenza analitica. Questo processo di traduzione non è una semplice sostituzione di termini, ma rappresenta la profonda ricontestualizzazione alla base di questo lavoro. Il principio di "autenticazione" deve evolversi in un sistema di "corroborazione graduata" che accetta e quantifica l'incertezza. La "catena di custodia" deve trasformarsi in una "tracciabilità analitica" che garantisca il rigore intellettuale del processo di ragionamento. E il concetto di "prova" deve essere sostituito da quello di "indicatore", un frammento di informazione il cui significato è interpretato nel contesto di molteplici ipotesi. È attraverso questa traduzione che un quadro progettato per la giustizia può diventare uno strumento per l'Intelligence e al contempo consentire una riattualizzazione dell'intero ciclo di Intelligence da fonti aperte.



IL QUADRO DI ADATTAMENTO

Riconosciuta la necessità di una trasposizione concettuale, è ora possibile delineare formalmente i pilastri di un quadro adattato che definisco il “Protocollo per l'integrità analitica”. Questo protocollo reinterpreta i principi fondamentali del Protocollo di Berkeley, integrandoli con metodologie e strumenti specifici del mondo dell'Intelligence per creare un sistema coeso, pratico e rigoroso, progettato per aumentare la qualità, la trasparenza e la difendibilità delle valutazioni geopolitiche.

L’obiettivo è fornire agli analisti una cornice metodologica che consenta di valutare informazioni provenienti da fonti aperte in modo rigoroso, ma flessibile, riconoscendo la presenza costante dell’incertezza e la necessità di attribuire livelli di confidenza graduati ai dati raccolti.

I principi di questo protocollo si fondano sul concetto di corroborazione probabilistica, sulla tracciabilità analitica e sull’interpretazione contestuale degli indicatori. Attraverso questa impostazione, ogni valutazione diventa non solo più difendibile, ma anche più utile per chi deve prendere decisioni complesse in scenari geopolitici mutevoli. Il protocollo, quindi, non si limita a trasporre regole giuridiche nell’ambito Intelligence, ma le reinterpreta in chiave analitica, offrendo una guida pratica per affrontare le sfide della moderna raccolta e valutazione delle informazioni.

Corroborazione graduata (adattamento dell'autenticazione)

Il primo principio affronta la natura intrinsecamente incerta dell'informazione nel dominio dell’OSINT. Mentre il Protocollo di Berkeley si concentra sulla verifica binaria (un'informazione è autentica o non lo è), il Protocollo per l'integrità analitica introduce un approccio probabilistico. L'obiettivo non è raggiungere una certezza assoluta, ma assegnare un livello di confidenza ponderato a ogni singola informazione.

Questo principio sposta l'enfasi dalla semplice verifica alla corroborazione graduata. Invece di scartare un'informazione perché non può essere autenticata al 100%, l'analista la valuta secondo tre fattori prioritari:

1) Affidabilità della fonte

Si valuta la reputazione storica e la potenziale parzialità della fonte. Un comunicato stampa ufficiale di un governo, pur essendo potenzialmente propagandistico, ha un'origine diversa e più tracciabile rispetto a un post di un account social media anonimo. Un'immagine satellitare commerciale ha un'affidabilità intrinseca superiore a una foto a bassa risoluzione di provenienza sconosciuta.

2) Credibilità dell'informazione

Si valuta la plausibilità dell'informazione nel contesto di altri indicatori noti. Un'informazione, anche se proveniente da una fonte di dubbia affidabilità, può acquisire credibilità se è coerente con dati provenienti da molteplici altri flussi informativi indipendenti.

3) Valutazione dell'impatto percettivo

Questo terzo fattore, fondamentale nell'odierno ambiente informativo, valuta la potenziale risonanza di un'informazione, indipendentemente dalla sua veridicità. Un'informazione, anche se falsa o non verificata, può diventare un "fatto politico" o "sociale" se ha un impatto significativo sulla percezione dei diversi attori.

L'analisi deve quindi considerare:

- impatto sull'opinione pubblica: l'informazione è sufficientemente scioccante, emotiva o virale da poter generare panico, indignazione o un forte sostegno a una causa, mettendo così pressione sui decisori?
- impatto sui decisori: l'informazione, vera o falsa che sia, costringerà un leader politico o militare a reagire pubblicamente per gestire la percezione, anche se le sue fonti di Intelligence affermano il contrario?
- impatto sull'analista: l'informazione ha una tale carica emotiva (es. un video di atrocità) da poter innescare bias nell'analista stesso, come il bias di conferma o l'ancoraggio, compromettendone l'obiettività?

Questo processo richiede quella "valutazione critica delle fonti e delle informazioni" che peraltro è il cuore di ogni attività Intelligence. Il risultato non è un verdetto di "vero" o "falso", ma un giudizio analitico: "l'indicatore X (es. movimento di carri armati) ha un'alta attendibilità, essendo corroborato da immagini satellitari, dati di tracciamento ferroviario e molteplici video geolocalizzati da fonti diverse". Questo approccio permette di costruire un quadro informativo sfumato, dove ogni pezzo del puzzle possiede un valore di attendibilità chiaramente dichiarato.

Tracciabilità analitica (adattamento della catena di custodia)

Questo principio rielabora il concetto legale di "catena di custodia" per il processo di Intelligence. Se la catena di custodia legale garantisce l'integrità fisica di una prova, la tracciabilità analitica garantisce l'integrità intellettuale di una conclusione. È un percorso trasparente e verificabile che conduce dal dato grezzo open source alla valutazione finale di Intelligence, permettendo a un supervisore, a un collega o a un futuro analista di riesaminare e, se necessario, contestare ogni passo del ragionamento.

Per aderire a questo principio, l'analista deve documentare meticolosamente:

- cosa: quali informazioni specifiche sono state raccolte (es. il testo di un tweet, un'immagine, un articolo);
- dove: la provenienza esatta dell'informazione (URL specifici, handle di social media, nome della pubblicazione);
- quando: la data e l'ora esatte in cui l'informazione è stata raccolta e archiviata;
- come: le metodologie e gli strumenti utilizzati per la raccolta, la conservazione e la verifica (es. "geolocalizzato utilizzando Google Earth e Sentinel Hub", "cronolocalizzato tramite analisi delle ombre con SunCalc").

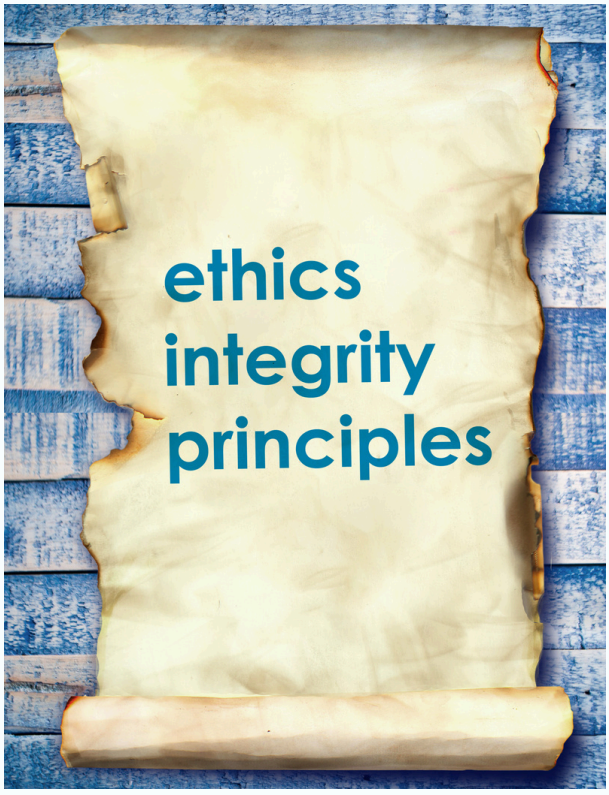
L'implementazione pratica di questo principio è resa possibile e significativamente più efficiente da strumenti specializzati che consentono di catturare, archiviare, marcare temporalmente e calcolare l'hash di ogni singola pagina web visitata durante un'indagine. Ciò consente di creare automaticamente una "traccia di controllo trasparente" che costituisce la spina dorsale della tracciabilità analitica. Inoltre, permette all'analista di "mostrare il proprio lavoro" con una precisione forense, eliminando l'ambiguità e rafforzando la riproducibilità e la credibilità dell'intero processo analitico.

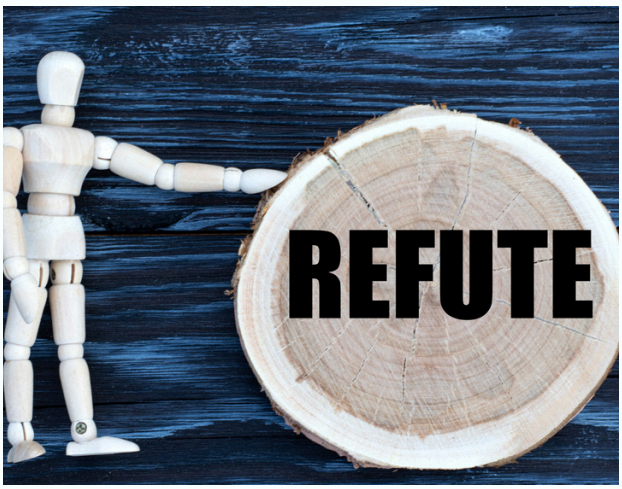
Responsabilità etica (adattamento della protezione)

Questo principio amplia il perimetro etico del Protocollo di Berkeley per affrontare le sfide uniche del dominio Intelligence.

Mantiene il dovere fondamentale di proteggere fonti, testimoni e individui da danni fisici e psicologici, ma aggiunge due dimensioni rilevanti:

Privacy by design: il principio impone una considerazione proattiva e sistematica della privacy. Riconosce che, anche se i dati sono pubblici, la loro aggregazione e analisi su larga scala possono creare profili dettagliati e intrusioni significative nella sfera privata degli individui. Per affrontare questo rischio, il protocollo adattato raccomanda l'integrazione di quadri di valutazione come l'OSINT Privacy Impact Framework (OPIF). L'OPIF fornisce un processo strutturato per identificare, valutare e mitigare i rischi per la privacy in ogni fase del flusso di lavoro OSINT (raccolta, elaborazione, analisi e disseminazione), garantendo che le considerazioni sulla privacy siano integrate nel processo fin dall'inizio, non aggiunte come ripensamento.





Responsabilità dell'impatto: l'analista OSINT è tenuto a valutare attentamente le implicazioni strategiche derivanti dalla propria analisi. Un report OSINT non costituisce un documento accademico; rappresenta invece uno strumento fondamentale che supporta processi decisionali potenzialmente rilevanti in ambiti quali ad esempio: la politica diplomatica, le operazioni militari e le strategie aziendali. L'analista deve quindi essere consapevole di come la propria valutazione potrebbe essere interpretata, utilizzata o persino strumentalizzata nel contesto altamente politicizzato delle relazioni internazionali. Ciò include la chiarezza nell'esprimere i livelli di attendibilità e nel delineare le incertezze e le lacune informative.

Confutazione strutturata (analisi collaborativa e sfidante)

Questo è l'elemento che ritengo più distintivo del protocollo adattato. Affronta direttamente la più grande vulnerabilità dell'analisi di Intelligence: i bias. La sfida posta da "disinformazione e potenziali manipolazioni" è tanto più efficace quanto più riesce a sfruttare le predisposizioni e i preconcetti dell'analista.

Per contrastare questa minaccia interna, il principio della confutazione strutturata rende obbligatoria l'integrazione di una metodologia analitica rigorosa.

Sebbene l'Analisi delle Ipotesi Concorrenti (ACH) sia spesso citata come la tecnica di riferimento per questo scopo, la sua applicazione completa può risultare eccessivamente lunga e complessa in contesti operativi caratterizzati da sovraccarico informativo e tempi decisionali ristretti. Pertanto, questo protocollo propone un approccio alternativo, più agile e collaborativo: l'analisi collaborativa e sfidante. Questa metodologia combina la rapidità del brainstorming con il rigore delle tecniche di challenge analysis (analisi competitiva), come il Key Assumptions Check (verifica delle assunzioni chiave) e il Red Teaming.
L'obiettivo non è più valutare esaustivamente ogni possibile ipotesi contro ogni prova, ma testare la robustezza dell'ipotesi più probabile attraverso un processo di critica strutturata e adversarial thinking (pensiero contrastante).
Il processo si articola in tre fasi rapide:
1) brainstorming strutturato e formulazione dell'ipotesi di lavoro: un team di analisti, possibilmente con background diversi, si riunisce per una sessione di brainstorming focalizzata e a tempo. Utilizzando tecniche come il silent brainstorming (dove le idee vengono scritte individualmente prima di essere condivise), il gruppo genera rapidamente le possibili spiegazioni per un dato evento. L'obiettivo è identificare in breve tempo l'ipotesi più plausibile sulla base delle conoscenze iniziali, che diventerà l'ipotesi di lavoro;

2) identificazione delle assunzioni chiave: una volta definita l'ipotesi di lavoro, il team si pone una domanda fondamentale: "cosa deve essere assolutamente vero affinché questa ipotesi sia corretta?". Vengono elencate tutte le assunzioni implicite ed esplicite su cui si basa la tesi. Questo importante passaggio sposta il focus dalle prove a favore alle fondamenta logiche dell'argomentazione, spesso rivelandone i punti più deboli;

3) sessione di "Red Teaming" o "Avvocato del Diavolo": il team si divide idealmente in due sottogruppi:

- Blue team: ha il compito di difendere l'ipotesi di lavoro, utilizzando le prove disponibili;
- Red team: ha il compito di attaccare e smontare l'ipotesi di lavoro, agendo come un avversario intelligente. Il Red Team deve cercare attivamente prove contrarie, proporre interpretazioni alternative dei dati e mettere in discussione le assunzioni chiave identificate nella fase 2. Le domande guida per il Red Team includono: "come potremmo essere ingannati?", "quale informazione, se fosse vera, farebbe crollare la nostra tesi?", "l'avversario si sta comportando come ci aspettiamo o stiamo cadendo nel mirror-imaging?".

Questo approccio dinamico e collaborativo mitiga i bias più pericolosi in modo più efficiente rispetto a una matrice ACH completa. Nello specifico:

- il bias di conferma viene contrastato attivamente dal ruolo istituzionalizzato del Red Team, il cui unico scopo è cercare prove che confutino l'ipotesi dominante.
- la struttura “adversarial” del dibattito incoraggia il dissenso costruttivo e contrasta il pensiero di gruppo, evitando al contempo di convergere prematuramente su una conclusione comoda ma non verificata.

Questo metodo non solo impone una disciplina intellettuale, ma promuove anche la flessibilità mentale, preparando gli analisti a riconsiderare rapidamente le proprie conclusioni qualora emergessero nuove informazioni. Rende il processo di ragionamento esplicito e difendibile, trasformando il giudizio da un'arte intuitiva a un processo di stress test strutturato.

IMPLEMENTAZIONE E IMPERATIVI STRATEGICI

L'introduzione del Protocollo per l'integrità analitica non può rimanere un esercizio puramente teorico. Per realizzare il suo potenziale trasformativo, è necessaria un'implementazione deliberata e strategica da parte di tutti gli attori che operano nell'ecosistema dell'Intelligence da fonti aperte. Questa sezione fornisce raccomandazioni attuabili, differenziate per i principali stakeholder, con l'obiettivo di tradurre i principi del protocollo in prassi operative, standard formativi e capacità tecnologiche.

Per le agenzie di Intelligence e gli organismi governativi

Per le entità statali, l'implementazione del protocollo adattato costituisce un'opportunità per incrementare la professionalità delle competenze OSINT, elevando al contempo sia la qualità sia la difendibilità dei prodotti di Intelligence.

Integrazione dottrinale: il primo passo consiste nell'integrare il Protocollo per l'integrità analitica nella dottrina ufficiale e negli standard professionali (tradecraft). Ciò implica la formalizzazione dei principi di corroborazione graduata, tracciabilità analitica, responsabilità etica e confutazione strutturata come requisiti imprescindibili nelle valutazioni OSINT. Tale approccio si allinea al modello NATO, finalizzato allo sviluppo di un "sistema OSINT olistico" che coniughi personale altamente qualificato, processi standardizzati e strumenti tecnologicamente avanzati.

Riforma della formazione: i programmi formativi destinati agli analisti necessitano di un'evoluzione sostanziale. È ormai insufficiente limitarsi all'insegnamento dell'utilizzo di tool OSINT: i curricula devono prevedere moduli approfonditi su metodologie analitiche strutturate e su quadri etici quali l'OPIF. Gli analisti devono acquisire competenze non solo nell'identificazione delle informazioni, bensì anche nel pensiero critico, con particolare attenzione al riconoscimento e alla gestione dei bias.

Investimenti tecnologici mirati: Le scelte in materia di acquisizione tecnologica dovrebbero essere orientate dai principi sanciti dal protocollo.

Occorre dare priorità a soluzioni che favoriscano la tracciabilità analitica, a piattaforme collaborative che agevolino la revisione tra pari e l'analisi collaborativa e sfidante, nonché a sistemi basati sull'intelligenza artificiale sviluppati per supportare l'analista nell'individuazione di pattern e anomalie, mantenendo comunque il ruolo centrale dell'intervento umano per garantire giudizio critico e supervisione etica.

Per la comunità OSINT indipendente (giornalisti, ONG, ricercatori)

Per gli attori non statali, che spesso operano con risorse più limitate, ma con un impatto pubblico significativo, il protocollo offre un percorso per massimizzare la credibilità e l'influenza del loro lavoro.

Adottare la trasparenza metodologica: la trasparenza non è una debolezza, ma un punto di forza. Pubblicando non solo le conclusioni, ma anche i metodi e i dati utilizzati, si costruisce fiducia con il pubblico e si rende il proprio lavoro resistente alle critiche e alle campagne di discredito. L'adozione dei principi di tracciabilità analitica e confutazione strutturata dovrebbe diventare uno standard per le indagini pubbliche di alto profilo.

Collaborazione e standard comunitari: la comunità OSINT indipendente dovrebbe sfruttare le piattaforme collaborative per promuovere l'adozione di questi standard. La revisione tra pari delle analisi, la condivisione di best practice e lo sviluppo di linee guida etiche comuni possono elevare la qualità complessiva del lavoro prodotto dall'intero settore, rafforzandone la legittimità agli occhi dei decisori politici e del pubblico.

Per l'ambito Corporate e la Business Intelligence

Nel settore privato, l'adozione del "Protocollo per l'integrità analitica" è una questione di sopravvivenza strategica e vantaggio competitivo. Le aziende globalizzate sono esposte a rischi geopolitici che possono avere un impatto diretto e devastante sul bilancio. L'implementazione del protocollo all'interno dei team di corporate Intelligence, risk management e due diligence è quindi un imperativo.

Resilienza della catena di approvvigionamento: le aziende devono anticipare le interruzioni. Applicando la corroborazione graduata, un team di OSINT aziendale può valutare l'affidabilità delle notizie su disordini civili, scioperi o instabilità politica in una regione dove si trovano fornitori chiave.

Gestione del rischio di mercato e Due Diligence: prima di un investimento, di una fusione o di un'acquisizione (M&A), è essenziale comprendere il rischio politico, reputazionale e normativo. La tracciabilità analitica diventa fondamentale per costruire un dossier difendibile che mappi le connessioni di un potenziale partner con entità sanzionate, Politically Exposed Persons (PEPs) o la sua esposizione a violazioni dei diritti umani (fattori ESG). Un'analisi rigorosa può prevenire danni reputazionali e sanzioni legali.

Protezione degli asset e del personale: le aziende con personale espatriato o infrastrutture in regioni instabili possono utilizzare il protocollo per produrre valutazioni di minaccia affidabili. L'analisi collaborativa e sfidante permette di testare le assunzioni sulla sicurezza di una determinata area, sfidando la "normalità" percepita e identificando indicatori di un deterioramento della sicurezza prima che si verifichi un incidente.

Per le aziende, l'adozione di questo protocollo trasforma l'OSINT da una semplice attività di monitoraggio a una funzione di Intelligence strategica, essenziale per proteggere gli investimenti, garantire la conformità e navigare con successo in un mercato globale sempre più incerto e frammentato.

Facilitatori tecnologici ed educativi

L'implementazione su larga scala del protocollo dipende anche da un ecosistema di supporto più ampio e in particolare:

- sviluppo di strumenti accessibili: è necessario continuare a sostenere lo sviluppo e la diffusione di strumenti OSINT, sia commerciali che open-source, che incorporino i principi del protocollo. Ciò include strumenti di archiviazione e conservazione, piattaforme di analisi geospaziale a basso costo e software che facilitino l'applicazione delle metodologie analitiche;
- integrazione accademica: le istituzioni accademiche hanno un ruolo fondamentale da svolgere. I corsi di laurea in relazioni internazionali, studi sulla sicurezza, giornalismo e informatica dovrebbero integrare moduli obbligatori sull'analisi OSINT, sull'analisi strutturata e sull'etica digitale. Garantire che la futura generazione di analisti, diplomatici e giornalisti sia formata solidamente su questi principi rappresenta un investimento strategico di lungo periodo per elevare la qualità del dibattito pubblico e dei processi decisionali su scala globale.

SVILUPPO DI UNO STANDARD DI RIFERIMENTO PER L'ANALISI OSINT

Partendo dal Protocollo di Berkeley questo lavoro cerca di proporre uno standard professionale aggiornato per l'utilizzo dell'OSINT nell'ambito delle attività di analisi. La tesi fondamentale è che la crescente centralità dell'Intelligence da fonti aperte nel processo decisionale strategico richiede un corrispondente e commisurato aumento del rigore analitico.

Non è più sufficiente essere abili nella raccolta di informazioni; è imperativo essere disciplinati e trasparenti nel loro giudizio.

È stato dimostrato che i principi fondamentali del Protocollo di Berkeley, originariamente sviluppato per soddisfare le rigorose esigenze dell'ambito legale, possono essere efficacemente applicati anche nel contesto complesso e incerto della geopolitica al fine di promuovere la comprensione. Attraverso una trasposizione concettuale mirata, l'enfasi sull'autenticazione si evolve in una corroborazione graduata che gestisce l'incertezza; la necessità di una catena di custodia si trasforma in una tracciabilità analitica che garantisce l'integrità intellettuale; l'imperativo di protezione si espande in una responsabilità etica e la ricerca di oggettività viene rafforzata da una confutazione strutturata che combatte attivamente i bias.

Il "Protocollo per l'integrità analitica" qui proposto non rappresenta semplicemente un nuovo approccio metodologico, ma ha l'ambizione di voler rappresentare un manifesto per la professionalizzazione dell'analisi OSINT.

La sua applicazione comporta vantaggi concreti e rilevanti. Fornisce una difesa robusta e strutturata contro la crescente minaccia della disinformazione e dell'inganno strategico, che prospera sull'analisi intuitiva e non strutturata. Mitiga i rischi intrinsechi e pervasivi dei bias, che rappresentano la più grande vulnerabilità di ogni analista. Infine, promuove una maggiore fiducia nei prodotti di Intelligence che informano le decisioni più critiche del nostro tempo, rendendo il processo di ragionamento trasparente, difendibile e verificabile. Sono convinto sia il passo necessario per garantire che l'OSINT si distingua per maggiore trasparenza, accuratezza metodologica e una più solida capacità di elaborazione strategica.

DECALOGO PER L'ANALISTA OSINT

1

Non fidarti mai di una singola fonte

La corroborazione è il fondamento della credibilità. Un'informazione, per quanto plausibile, rimane un'illazione finché non è confermata da almeno due o tre fonti indipendenti e non correlate.

2

Valuta la fonte prima del contenuto

Ogni informazione porta con sé il suo "DNA". Chiediti sempre: chi sta parlando? Qual è la sua reputazione storica? Qual è il suo potenziale bias o la sua agenda? L'affidabilità della fonte è il primo filtro di validità.

3

Considera l'impatto, non solo la veridicità

Un'informazione non deve essere vera per essere strategicamente rilevante. Valuta sempre il suo potenziale impatto percettivo sull'opinione pubblica, sui decisori e su te stesso. Una narrazione virale, anche se falsa, può diventare un fatto.

4

Archivia ogni passo della tua analisi

La tua memoria è fallibile, internet è volatile. Usa strumenti per creare una traccia forense del tuo lavoro: cosa hai visto, dove e quando. La tracciabilità è la tua difesa contro eventuali contestazioni.

5

Rendi il tuo ragionamento replicabile

Un'analisi valida è un'analisi il cui processo può essere seguito e verificato da altri. Documenta le tue metodologie e le tue scelte. La trasparenza non è una debolezza, ma la più alta forma di rigore intellettuale.

6

Rispetta la privacy anche nel dominio pubblico

Il fatto che un'informazione sia pubblica non ti dà il diritto di abusarne. Applica sempre i principi di minimizzazione dei dati e chiediti se la raccolta di un'informazione personale è strettamente necessaria per il tuo obiettivo.

7

Sii consapevole del peso delle tue conclusioni

La tua analisi non è un esercizio accademico; informa decisioni che hanno conseguenze reali. Comunica sempre con chiarezza i livelli di probabilità, le incertezze e le lacune informative. La responsabilità è parte integrante del mestiere.

8

Sii il primo e più severo critico di te stesso

Il tuo avversario più insidioso non è la disinformazione esterna, ma il tuo stesso bias. Sii ossessionato dal riconoscere le tue predisposizioni (bias di conferma, di ancoraggio) e dal combatterle attivamente.

9

Identifica e metti in discussione le tue assunzioni

Ogni analisi si fonda su assunzioni implicite. Prima di difendere una conclusione, chiediti: "Cosa sto dando per scontato?". Esplicita queste assunzioni e testane la validità. Un'assunzione errata è il punto di rottura di ogni catena logica.

10

Cerca attivamente prove che smentiscano la tua ipotesi principale

Non innamorarti della tua tesi. Istituzionalizza il dissenso: agisci come "avvocato del diavolo" o crea un "Red Team" il cui unico scopo è smontare la tua argomentazione. Un'ipotesi che sopravvive a un serio tentativo di falsificazione è un'ipotesi robusta.