

L'Open Source Intelligence nella prospettiva NATO

Carlo Centoducati

INDICE

Introduzione.	pg. 3
	pg. 3
I. L'intelligence delle fonti aperte.	pg. 4
II. Definizioni.	pg. 4
III. Le fonti dell'OSINT.	pg. 6
IV. La direzione dell'OSINT.	pg. 7
V. Il ciclo dell'intelligence applicato alle fonti aperte.	pg. 7
V, 1. Scoperta: selezione ed interrogazione delle fonti.	pg. 9
V, 2. Discriminazione.	pg. 9
V, 3. Distillazione.	pg. 11
V, 4. Diffusione.	pg. 12
VI. Conclusioni.	
	pg. 13
Bibliografia	

Introduzione

Gli ultimi due decenni sono stati caratterizzati da una serie di mutamenti epocali. Il crollo sovietico, infatti, ha determinato una profonda trasformazione degli assetti geopolitici e strategici globali, e la rivoluzione tecnologica ha compresso come mai prima le distanze tra luoghi e persone un tempo molto lontani tra loro.

A questi due elementi sono inoltre andati sommandosi una lunga serie di dinamiche innovative e di eventi, purtroppo ben conosciuti, in parte da essi derivati.

La nuova dimensione degli equilibri internazionali, caratterizzata dall'unipolarismo statunitense sul cui conto molti si interrogano, ha d'altro canto mostrato la faccia più preoccupante dell'assenza di un ordine mondiale stabile, del proliferare di armi di distruzione di massa e di conflitti interni su base etnico-religiosa, spesso accompagnati da gravi violazioni dei diritti umani e dal preoccupante problema dei rifugiati e degli sfollati. Più recentemente, la minaccia del terrorismo internazionale ha letteralmente rivoluzionato l'agenda politica globale, determinando una profonda revisione dei concetti di difesa e di sicurezza nazionale, l'emergere di nuove dottrine strategiche "aggressive" ed il verificarsi di conflitti interstatuali.

Nel frattempo, l'invenzione del "world wide web" e la diffusione dell'accesso ad internet, virtualmente disponibile a basso costo e con notevole semplicità in ogni parte del mondo, hanno determinato una altrettanto repentina rivoluzione nel mondo dell'informazione e della conoscenza, consentendo ai singoli individui di ottenere e scambiare informazioni con l'intera platea globale in modo immediato, economico e sostanzialmente libero da qualsiasi controllo. Non ultimo, internet contribuisce, assieme ad altri fenomeni come l'ulteriore riduzione dei costi di trasferimento e trasporto aereo o la crescente interdipendenza dei mercati globali, alla formazione di una cultura globale e di molte culture ad essa antagoniste, determinando nuove dinamiche nei fenomeni di integrazione e di contrapposizione tra individui e tra Stati.

Questo innovativo contesto apre e segna indelebilmente il nuovo millennio con innumerevoli sfide, pericoli ed opportunità fino a pochi anni orsono impensabili. Nell'accelerazione generalizzata che caratterizza la politica, l'economia e la cultura del nostro tempo, alcuni elementi storicamente considerati di secondo piano tornano sotto i riflettori. Nuova attenzione viene infatti focalizzandosi, negli ambienti legati alla difesa ed alla sicurezza dei diversi Paesi, sull'importanza dell'intelligence e sulle sue possibili evoluzioni. Nell'ambito di questo dibattito, un posto di particolare rilievo, soprattutto nei Paesi nordeuropei ed anglosassoni, è attribuito alla rivalutazione dell'intelligence delle fonti aperte (OSINT/OSI – Open Source Intelligence).

L'intelligence delle fonti aperte

Non esiste ancora, né in Italia né in altri Paesi, una definizione dell'intelligence delle fonti aperte che risulti unanimemente condivisa¹. In ambito NATO, per adottare il punto di vista attualmente più interessante sulla questione, l'open source intelligence è definibile come un processo di raccolta, selezione, distillazione e diffusione di informazioni non classificate ad una comunità ristretta di operatori ed in relazione a specifici argomenti². L'OSINT costituisce un punto di partenza, un indicatore importante per altre forme d'intelligence, e quando applicata in modo sistematico può ridurre drammaticamente la domanda di intelligence classificata limitandone il bisogno alle sole questioni che non possono trovare una risposta in modi più economici e legittimi.

L'OSINT è qualcosa di profondamente diverso dalla ricerca accademica, economica o giornalistica, nella misura in cui fa uso di strumenti d'intelligence di provata efficienza applicandoli ad una più ampia tipologia di fonti. In particolare, il tratto che maggiormente caratterizza l'open source intelligence è il fatto di essere un processo concepito non per acquisire o generare conoscenza, quanto piuttosto per mettere uno o più individui nelle condizioni di svolgere al meglio il proprio

lavoro attraverso la predisposizione delle sole informazioni necessarie. Nell'ambito di una coalizione, ciò risulta particolarmente utile per consentire a tutte le componenti nazionali di acquisire un punto di vista comune in relazione all'area delle operazioni (AoO – Area of Operations), ma anche per consentire alla coalizione stessa di dialogare in modo più efficace e fruttuoso con le organizzazioni civili che operano in quel contesto.

Le fonti aperte, come è noto, non sono un settore di pertinenza esclusiva dell'intelligence ma molto più familiare ad altri ambienti. La comunità dell'intelligence mondiale ha in parte già percorso i tempi³, e gli staff intelligence sia nazionali che NATO dovrebbero cercare di interfacciarsi al meglio con questo tipo di fonti, per consentire a chi ne ha bisogno di accedere ad informazioni di carattere rilevante senza richiedere autorizzazioni particolari. Si tratta di una necessità che si avvia a divenire sempre più cruciale nel tempo, nella misura in cui i vecchi, solidi e monolitici principi guida dell'intelligence tradizionale si trovano a dover fare i conti con una struttura della Difesa e della sicurezza che il nuovo contesto globale vuole più dinamica, dispersa e collaborativa⁴. La NATO si trasforma e si integra nelle relazioni internazionali divenendo un forum ampio ed un *sistema* di alleanze, mentre il terrorismo globale rende i sistemi-Paese più vulnerabili e quindi più integrati, esigendo che comparti una volta estranei dialoghino tra loro.

Il dialogo, nell'intelligence, è sempre stato un elemento problematico: non solo gli Stati hanno sempre manifestato una certa ritrosia nello scambiarsi informazioni classificate per la necessità di proteggere i propri interessi, le proprie procedure e non ultimo le proprie fonti⁵, ma anche al proprio interno hanno sempre vissuto un'ampia frattura tra la vita quotidiana della società civile ed il lavoro discreto dei servizi di sicurezza. Non è difficile, in questi presupposti, comprendere quanto la NATO sia stata danneggiata, nel corso degli anni, dall'impossibilità di generare al proprio interno processi sistematici atti a far circolare le informazioni. Questa situazione è destinata a cambiare, ma si pone il problema di come far coesistere un ampio bisogno di comunicazione con tutti i problemi connessi alla protezione delle informazioni sensibili. L'intelligence delle fonti aperte, la sua diffusione ed il suo interscambio, sembrano costituire la miglior risposta a quest'esigenza.⁶

Affinché l'OSINT possa dare i suoi frutti, tuttavia, alle fonti aperte dovrebbero essere applicati i tradizionali processi, di ormai provata efficacia, relativi al trattamento delle informazioni nell'intelligence tradizionale, al fine di garantire una maggiore qualità dei dati in uscita ed alimentare al meglio la il successivo assemblaggio di prodotti che integrano informazioni provenienti dalle varie componenti intelligence (all-source intelligence), fornendo una guida ed una solida base informativa per gli staff nazionali quanto per quelli multinazionali.

Per questo motivo è necessario accostarsi all'OSINT come ad una disciplina scientifica; in questo senso, si possono identificare almeno quattro elementi da tenere in considerazione: le definizioni, le fonti, la direzione ed il ciclo dell'OSINT.

Definizioni

Parlare di open source intelligence vuol dire identificare non un processo ma un prodotto, occorre dunque fare alcune distinzioni di base tra *dati da fonti aperte* (Open Source Data, ossia tutto il sistema di fonti primarie cui fare riferimento, come fotografie, documenti interni, registrazioni audiovideo, immagini satellitari e debriefing orali), *informazioni da fonti aperte* (Open Source Informations, dati grezzi secondari emersi nel processo di analisi delle OSD tramite filtraggio e verifica, di solito disponibili ad un ampio spettro di consumatori nella forma di report specialistici, quotidiani, libri), *intelligence delle fonti aperte* (OSINT, ossia informazioni derivanti da un processo volontario di scoperta, selezione, distillazione e distribuzione ad una categoria selezionata, per rispondere a particolari bisogni informativi utilizzando gli strumenti propri dell'intelligence) ed *OSINT verificate* (OSINT-V, cui può essere attribuito il più alto livello di aderenza alla realtà. E' il prodotto finale dell'OSINT, destinato al confronto con informazioni classificate nel processo di *all-source intelligence*)⁷.

Le fonti dell'OSINT

L'ampio e variegato sistema di fonti relativo all'OSINT è composto da tutti quei dati, in forma cartacea, elettronica oppure acquisiti oralmente, accessibili legalmente sia in modo gratuito che a pagamento, di solito attingendo dal mondo pubblico e privato della vita civile. Indubbiamente, come già detto, internet è attualmente sotto la lente d'ingrandimento non solo degli analisti che in molti modi utilizzano il web per il proprio lavoro, ma anche dei teorici dell'intelligence, impegnati a stabilire funzioni e criteri, opportunità e rischi, strumenti e procedure sicure⁸. Digitando una parola-chiave in qualsiasi motore di ricerca, si può accedere a milioni di pagine web contenenti altrettanti collegamenti ad ulteriori fonti; imparando ad utilizzare i sistemi di ricerca avanzata si possono effettuare ricerche più mirate, conferendo un primo elemento di scientificità all'analisi. In questo senso, tuttavia, non si deve incorrere nell'errore di accostarsi con eccessiva superficialità alla ricerca in rete, attribuendole un valore assoluto, una sicurezza data oppure una semplicità che è solo apparente. Dei milioni di informazioni cui è possibile accedere attraverso internet solo alcune sono utili ai fini dell'intelligence, e la loro identificazione non è affatto facile. Per citare solo i limiti più evidenti di questo tipo di ricerche, gli analisti si confrontano quotidianamente con l'impossibilità di leggere, controllare e verificare tutte le pagine disponibili, di identificare l'autore, la data (e l'ora) di molte notizie, di stabilire, in molti casi, l'imparzialità della fonte ed i suoi obiettivi,⁹ oppure con grosse difficoltà nel consultare e comprendere informazioni in varie lingue. Ciò per restare nel vago, poiché approfondendo si potrebbero enucleare molti altri fattori, come il tempo necessario a dare a tutte le informazioni un formato standard ed immediatamente comprensibile, il bisogno, spesso essenziale, di navigare nella rete in modo più o meno anonimo, le misure di contro-intelligence (*deception* - inganno) con le quali è possibile scontrarsi¹⁰.

Oltre ad internet, il mondo delle fonti aperte comprende un'ampia serie di fonti più "tradizionali" tra le quali un posto di rilievo spetta senza dubbio ai servizi d'intelligence forniti da organizzazioni private. Alcune tra queste organizzazioni sono molto ben conosciute ed operano da decenni selezionando, verificando, formattando, indicizzando, riassumendo e presentando informazioni rilevanti, e da alcuni anni hanno amplificato la propria importanza ed il proprio business rendendo disponibili varie tipologie di servizi online. Independent Information Brokers, Lexis-Nexis, Dialog, Jane's Group, Reuters¹¹ sono solo alcune tra le più conosciute agenzie di questo tipo, e forniscono servizi sia attraverso il pagamento della singola analisi che con tariffe *flat* calcolate su un numero di accessi predefinito sia infine sulla base del tempo di consultazione di cui il cliente usufruisce in un determinato periodo.

A causa dell'alto costo di questi servizi, sarebbe opportuno che gli analisti conoscessero molto bene i loro meccanismi di funzionamento e strutture di costo per evitare errori o duplicazioni che possono rivelarsi molto costose. In alternativa, la NATO ipotizza il ricorso alla consulenza di esperti in archivistica¹², ma è ovvio che questa ipotesi è più remota e difficile da implementare.

All'interno di questa tipologia di fonti, non bisogna sottovalutare il peso crescente dei servizi commerciali impegnati nella fornitura di immagini satellitari, in grado di fornire materiale sempre più dettagliato a costi sempre più accessibili ed in una cornice giuridica internazionale che permette loro di immortalare qualunque cosa senza incorrere in alcuna sanzione. Questi servizi stanno rivoluzionando l'intelligence delle immagini¹³ (IMINT – Imagery Intelligence) ponendo non pochi quesiti ai Governi di molti Paesi.

Un'altra tipologia di fonti che nell'OSINT assume una grande importanza è quella della *cd. letteratura grigia* (Grey Literature), costituita da informazioni ottenibili legalmente ma in modo meno semplice, ad esempio attraverso il contatto diretto o l'uso di canali particolari¹⁴. Si tratta di materiale non pubblicato né distribuito, catalogato o diffuso se non in ambienti ristretti, ed include documenti interni, bozze, reports tecnici, documenti delle amministrazioni, dei sindacati, delle organizzazioni non governative e di altri soggetti.

Il più tipico dei servizi d'intelligence, quello umano (HUMINT – Human Intelligence) trova una valida controparte OSINT nel ricorso a persone che hanno un'esperienza diretta del campo o evento

di interesse (Overt Human Observers),¹⁵ molto utili soprattutto in relazione ad eventi o luoghi (si pensi ad alcuni Paesi africani) in relazione ai quali non è possibile ottenere altre informazioni¹⁶. Gli individui restano sempre il fattore in grado di fornire il servizio più completo ed economico, ma è ovvio che solo in certe situazioni il loro apporto può essere utilizzato in condizioni di sicurezza e di legalità. Distinti dagli osservatori sono gli esperti (Overt Human Experts)¹⁷, ad esempio nel settore degli studi strategici, il cui contributo può essere richiesto a pagamento presso università, centri studi, organizzazioni governative e non, anche attraverso l'uso di database e servizi disponibili su internet.

Adottando un altro punto di vista, ci si può concentrare sui soggetti dai quali è possibile attingere informazioni utili al processo di open source intelligence. I servizi di sicurezza nazionali, ad esempio, pur non essendo direttamente coinvolti nel soddisfacimento dei requisiti OSINT possono alimentarne sensibilmente il processo, fornendo informazioni non classificate già sottoposte ad analisi intelligence. A questo proposito, vale la pena di ricordare come alcuni Paesi (Stati Uniti, Olanda, Danimarca, Norvegia e Gran Bretagna, ma altri Stati dispongono di capacità minori in rapida crescita) siano eccezionalmente abili nel maneggiare informazioni di questo tipo, disponendo peraltro di cellule OSINT perfettamente integrate nella propria struttura nazionale di all-source intelligence.

Risaputamente, le Ambasciate e tutte le altre tipologie di missioni diplomatiche costituiscono da sempre una eccezionale fonte di OSINT a basso costo, soprattutto quando vengono interessate direttamente da compiti specifici. E' ovvio che si tratta di istituzioni cui non spetta un preciso dovere di rispondere a quesiti posti da cellule OSINT nazionali o NATO, ma un certo livello di coordinamento, anche informale, è suscettibile di produrre ripercussioni positive e di ampia scala sul processo d'intelligence.

Da non dimenticare, inoltre, le Camere del Commercio, ampiamente diffuse nella maggiore parte dei Paesi e generalmente ritrovo di piccole comunità manageriali altamente specializzate e perfettamente informate, spesso di estrazione internazionale e comunque in grado di fornire informazioni preziose anche su argomenti di scala non propriamente nazionale. Un contatto informale con queste istituzioni, soprattutto nelle aree in cui i contingenti vengono dispiegati sul terreno, può risultare di grande utilità.

Menzione particolare va inoltre riservata alle organizzazioni internazionali, non governative e religiose, la cui diffusione ha ormai raggiunto livelli di capillarità tali da configurarsi come un'eccellente, in potenza, rete informativa globale. Le agenzie delle Nazioni Unite, il Comitato Internazionale della Croce Rossa, Medici Senza Frontiere, l'Opus Dei, l'Islamic World Foundation e molte altre organizzazioni hanno sedi in ogni angolo del mondo e quotidianamente sperimentano il contatto con le realtà locali, disponendo di informazioni il cui diretto accesso è spesso precluso ad altre categorie di osservatori.

La direzione dell'OSINT

Una buona conoscenza del ciclo dell'intelligence costituisce un requisito fondamentale posto alla base della consultazione di fonti pubbliche e commerciali ai fini dell'OSINT, attraverso l'uso di strumenti legali e generalmente a basso costo, utili soprattutto laddove sia necessario rispondere rapidamente a richieste specifiche e non sia possibile farlo in sicurezza attraverso i sistemi tradizionali.

Come è noto, in ambito NATO spetta al Comandante la definizione dei requisiti essenziali di informazione (EEI - Essentile Elements of Information) e la costituzione degli assetti intelligence utili a soddisfarli. In questo contesto, l'OSINT non è necessariamente un servizio fornito su base nazionale né un elemento la cui collocazione debba risultare obbligatoriamente predeterminata. Generalmente, infatti, la cellula OSINT è subordinata alla cellula intelligence (CJ2 - Combined Joint Intelligence Cell), ma è evidente che altri elementi dello staff, come i comandanti delle cellule cooperazione civile-militare (CIMIC - Civil-Military Cooperation), gli addetti alle pubbliche

relazioni (PIO - Public Information Officers), la Polizia Militare ed altri, possono contribuire al suo lavoro come fossero una sorta di consiglio informale a disposizione del comandante.

I comandanti ed i loro staff devono valutare con grande attenzione le informazioni di cui hanno bisogno, articolando in modo puntuale e conciso le proprie richieste. Non è infrequente, infatti, che le richieste di informazioni (RfI – Request for Information) siano ampie o che addirittura vengano richiesti dei vaghi punti di situazione. Ciò può costituire un limite importante da superare, perché negli intenti del comandante si incardinano il recepimento e la comprensione delle sue intenzioni, due fattori fondamentali nella determinazione della tipologia e dell'ampiezza delle informazioni da ricercare.

L'OSINT è uno strumento formidabile per soddisfare queste richieste o comunque per fornire una guida nella ricerca di informazioni attraverso altri sistemi, ma non può essere appesantita dal bisogno di scremare cosa è realmente utile al comandante da cosa non lo è. Attraverso le fonti aperte possono infatti essere soddisfatti tanto i bisogni generici quanto quelli specifici,¹⁸ a patto che le linee guida fornite dall'alto siano esplicite. E' quindi un imperativo che i comandanti distinguano accuratamente le richieste generiche, come quelle relative alla fornitura di background storici o di informazioni generali utili alla pianificazione logistica e di altre branche, dai requisiti d'intelligence più accurati.

La pianificazione e la conduzione delle operazioni militari, infine, sono processi continui e ciclici, nei quali non è solo importante che i comandanti e gli staff richiedano informazioni, ma anche che sappiano interpretarle e valutarle correttamente. Affinché ciò possa avvenire nel miglior modo possibile, è fondamentale che il processo di comunicazione con tutte le componenti intelligence sia di tipo bi-direzionale, o in altri termini, che venga sempre fornito un feedback da parte di chi beneficia del prodotto-informazione nei confronti di chi lo ha elaborato.

Il ciclo dell'intelligence applicato alle fonti aperte

Poiché il bisogno di informazioni da parte della NATO è ampio, destinato a crescere significativamente nel tempo ed altamente dipendente dalle condizioni geopolitiche globali e dalle specifiche missioni, non è possibile pensare alla creazione di un database informativo permanentemente aggiornato da cui estrarre di volta in volta le informazioni ritenute utili. In questo senso, l'attenzione deve essere riposta non tanto sulle informazioni, quanto piuttosto sulle fonti e sui metodi utilizzati. Una conoscenza approfondita di questi due elementi, infatti, può consentire agli staff preposti alla produzione di OSINT di costruire rapidamente, ed in modo efficiente, processi di raccolta, discriminazione, distillazione e distribuzione di informazioni adeguati ai bisogni.

Il ciclo dell'intelligence si compone di quattro fasi principali (le cosiddette "four Ds": discovery, discrimination, distillation and dissemination¹⁹) suddivise in sottofasi a costituire un sistema molto complesso. In relazione al ciclo seguito, emergono le più sostanziali differenze tra l'intelligence tradizionale e l'OSINT, nella quale lo scambio informale sembra garantire prestazioni migliori rispetto alla predisposizione di *steps* gerarchicamente ordinati. Le quattro fasi dell'OSINT possono essere riassunte in una formula molto semplice: conoscere le fonti, apprendere nozioni sull'argomento, apprendere cosa è importante, comunicare con chi può trarne beneficio.

In realtà, il processo è molto più articolato e spesso abbastanza mutevole da non permettere facili semplificazioni. Diversamente da quanto avviene per altre forme d'intelligence, infatti, il ciclo dell'OSINT elaborato dalla NATO è tuttora in fase di formazione, ed al suo interno una certa flessibilità ed informalità è non solo accettata, ma addirittura stimolata. La cosa più utile da fare, stando così le cose, è procedere ad un'analisi dei fattori che, all'interno delle varie fasi, risultano di particolare interesse.

Scoperta: selezione ed interrogazione delle fonti.

Il primo passo alla base della costituzione di solide capacità OSINT è la costruzione di un sistema di fonti integrato e verificato, al fine di predisporre uno strumento di immediata e proficua utilizzazione nei periodi di crisi. Conoscere gli esperti, poter accedere facilmente ai loro ultimi

lavori, sapere di cosa si stanno occupando, poterli contattare, sono requisiti essenziali per il successo di tali iniziative. A questo proposito, l'Alleanza Atlantica ha deciso di costituire un vero e proprio inventario di esperti selezionati in base alle materie di competenza (SMEI - Subject-Matter Experts Inventory) sia presso propri comandi che a livello centralizzato. Grande attenzione viene inoltre riservata alla raccolta di informazioni sulle Camere di Commercio, sugli istituti di ricerca, le università, organizzazioni professionali ed organizzazioni non governative presenti nelle aree di interesse.

L'analisi OSINT deve sempre fare i conti con una serie di questioni ad essa strettamente correlate e di grande importanza. Tra queste, la sicurezza delle operazioni (OPSEC – Operation Security) nelle quali l'open source intelligence è inserita costituisce spesso un requisito nodale che può essere soddisfatto sia tramite l'uso di intermediari²⁰ che tramite particolari procedure di anonimizzazione, o di *randomizzazione*²¹ della navigazione internet. Inoltre, facendo l'OSINT ampio ricorso al contributo di organizzazioni esterne, uno strumento per proteggere la riservatezza delle ricerche effettuate può essere individuato nella stipula di accordi di segretezza (NDA – Non-Disclosure Agreements) la cui effettività è garantita dal significato economico che sottendono.

Accanto a questi imperativi di natura "interna", la collaborazione con agenti privati comporta anche una serie di vincoli giuridici derivanti dalle normative nazionali ed internazionali sul *copyright*. Alcuni governi, a tale proposito, hanno deciso di escludere per legge la propria responsabilità in questo settore, ma si tratta di iniziative poco gradite dagli operatori e suscettibili di ridurre il loro interesse a fornire prodotti di qualità. Nell'ambito più specificamente NATO, sarebbe inoltre impossibile imporre a tutti i Paesi membri di prevedere simili privilegi per l'Alleanza, sia attribuendole particolari diritti che agendo come intermediari, a meno di non rallentare i processi di OSINT e di fare i conti con le inevitabili disparità che tali misure andrebbero a determinare. Quello del rispetto del copyright, secondo la dottrina NATO, è un presupposto al quale non possono essere poste riserve, soprattutto al fine di garantire e mantenere il più alto livello di flessibilità possibile, anche a costi maggiori.

In quanto organizzazione internazionale, inoltre, la NATO ha sempre dovuto fare i conti con i problemi di natura linguistica. In questo campo, i contingenti dispiegati fuori-area oggi sperimentano un crescente bisogno di servizi di traduzione non disponibili all'interno dell'Alleanza. Ciò implica la necessità di ricorrere ad addetti esterni, soddisfatta sia a livello nazionale che dall'Alleanza stessa, che infine direttamente dai contingenti. A questa pratica è legata l'esigenza di identificare gli esperti disponibili e di selezionare tra questi ultimi coloro cui può essere attribuita una soddisfacente certificazione di sicurezza (Security Clearance). I servizi nazionali, d'altra parte, hanno mostrato di essere raramente disposti a distogliere risorse così preziose concedendole alla NATO, determinando maggiori difficoltà nel reperimento di interpreti e traduttori di qualità.

Ora che il processo di adeguamento della NATO a queste nuove esigenze è in corso di realizzazione, è essenziale che questi bisogni vengano rapidamente identificati e comunicati ai livelli superiori, affinché possano essere inseriti nel Future Intelligence Architecture Plan di cui l'organizzazione si è munita per essere pronta ad affrontare le sfide del futuro. Il meccanismo NATO, infatti, è ancora lontano dal funzionare adeguatamente per i fini dell'OSINT: la stessa comunicazione con l'esterno, che per l'open source intelligence costituisce un presupposto irrinunciabile, talvolta è un fattore problematico per l'Alleanza, sia a causa di semplici difficoltà burocratiche nell'identificare gli esperti ed i loro settori di eccellenza sia per ristrettezze finanziarie sia per l'esistenza, in alcuni Paesi, di normative che ostacolano o vietano esplicitamente il contatto tra personale impiegato nell'intelligence ed esperti privati. Ciò è reso ulteriormente complicato dal fatto che l'architettura di Comando, Controllo, Comunicazione, Computing ed Intelligence (C4I) NATO in genere non permette né l'accesso routinario ad internet né, soprattutto, l'interscambio di informazioni tra internet ed i propri database classificati.

Discriminazione

Il cuore pulsante dell'intelligence è senza dubbio costituito dalla selezione delle informazioni, un processo nel quale gli information requirements vengono incrociati con le fonti disponibili alla ricerca di altre fonti e di risposte che porteranno all'elaborazione del prodotto finito. All'interno di questa fase, spetta allo staff intelligence di stabilire quali domande possono trovare una risposta attraverso le fonti conosciute e quali debbano essere "girate" ad altri attori. In ambito NATO, le richieste alle agenzie nazionali d'intelligence sono dette RFI (Requests for Information). Questo processo, a sua volta, implica l'adozione di una strategia pre-elaborata fondata sulla ricerca delle fonti migliori e delle informazioni più accurate.

Nel contesto NATO, in quanto complemento essenziale della all-source intelligence, l'OSINT contribuisce a questo processo in modo sostanziale.

La raccolta delle informazioni è in genere il risultato più immediato della traduzione di una RFI in uno sforzo dell'intelligence tradizionale. In ambito OSINT, invece, per quanto detto relativamente all'ampia gamma di fonti disponibili, lo sforzo principale è sempre diretto alla selezione ed all'eventuale integrazione. Esistono, in questo senso, almeno tre strategie applicabili, ciascuna particolarmente adatta a specifici contesti e necessità ma tutte egualmente valide.

La prima di queste strategie sovverte nettamente il metodo d'intelligence tradizionale e si basa su un processo cd. *analyst-driven*, generalmente molto efficace qualora i tempi non siano troppo ristretti e fondato sull'autonoma capacità dell'analista di discernere gli elementi utili in base alla sua conoscenza del problema e del fruitore delle informazioni. Una diversa strategia è invece utile qualora si renda necessario rispondere rapidamente ad eventi improvvisi ed imprevisti, in relazione ai quali il fattore tempo gioca un ruolo essenziale. In questi casi, si tende ad utilizzare strategie cd. *events-driven*, che richiedono uno sforzo informativo più accentuato e concentrato. Infine, esistono strategie cd. *scheduled* che ben si adattano ad attività più generali, come quelle basate sulla revisione e sull'aggiornamento periodico delle informazioni relative a specifici argomenti.

Come si è detto, a prescindere dalla strategia adottata è molto importante che questi processi siano di tipo bi-direzionale: in questo modo, non solo l'analista può essere messo nelle condizioni di fornire prodotti migliori, ma ampliando la propria conoscenza degli utilizzatori finali e dei loro bisogni può anche fornire un buon servizio analyst-driven e predisporre aggiornamenti ed approfondimenti su quesiti cui è già stata fornita una risposta.

Quando si effettua un'analisi, i due fattori di maggior rilievo da tenere in considerazione sono il tempo e le informazioni di cui si dispone. Questi due elementi possono entrare in conflitto qualora si disponga di troppo poco tempo o di poche informazioni, oppure quando il tempo disponibile tende ad essere speso per districarsi in una miriade di informazioni, peraltro spesso contrastanti tra loro. Il rischio più rilevante in tema di OSINT, inutile dirlo, è l'ultimo tra quelli appena citati. Internet e le altre fonti aperte sono infatti muniti di un grande potere di seduzione nei confronti degli analisti, che possono facilmente essere indotti a sprecare tempo collezionando moli eccessive di informazioni oppure a sacrificare troppo tempo nella validazione delle fonti a scapito dell'analisi e del livello di dettaglio.²² Come già detto, una parte di questo problema può essere risolta predisponendo un elenco aggiornato delle fonti in base alla loro disponibilità ed obiettività; l'altra va curata con la formazione.

Distillazione

La terza fase del ciclo dell'OSINT è quella della distillazione delle informazioni importanti da quelle meno importanti, inesatte oppure false. Lavorare con le fonti aperte, tuttavia, può nascondere mille insidie: non è difficile né raro che gli operatori dell'OSINT (OSO – Open Source Operators) commettano involontariamente degli errori oppure siano vittime di inganni.

D'altra parte, attribuire un valore d'intelligence ad informazioni ottenute da servizi informativi nazionali è una pratica diffusa ma fortemente sconsigliata negli ambienti più professionali. In questi

casi, tuttavia, gli analisti hanno sempre a disposizione il proprio background professionale ed una genericamente solida conoscenza dell'affidabilità delle fonti e dei suoi possibili interessi.

Ciò non è sempre vero per coloro che operano con le open sources, in cui la provenienza dell'informazione può variare considerevolmente e non sempre è possibile avere o procurarsi informazioni dettagliate sulle fonti. In questo settore, dunque, è necessario che gli operatori mantengano sempre il più alto livello di vigilanza e di sospetto nei confronti delle informazioni che gestiscono, al fine di mettersi al riparo perlomeno dagli errori e dai raggiri più comuni.

L'informazione, inoltre, non è mai un fatto: negli ultimi anni, in particolare, non solo l'informazione tende ad essere con sempre maggior frequenza improntata al sensazionalismo,²³ ma gli stessi processi d'intelligence talvolta scricchiolano sotto il peso della produzione di consenso.

Ciò si somma ad una serie di errori comuni che vanno dall'errata impaginazione dell'informazione all'assenza di dati accessori come la data o la fonte, o ancora alla mancata verifica della sua credibilità, piccoli e grandi errori che possono ridurre notevolmente l'effettività del processo di OSINT.

L'allora NATO-SACLANT (oggi Allied Command Transformation) ha elaborato, proprio a questo proposito, una serie di linee guida per i propri analisti, destinate non solo ad impedire che essi possano inciampare negli errori più comuni, ma anche a fornire validi strumenti per la verifica del contenuto dei siti internet. Di particolare interesse risulta notare come esistano un buon numero di *tools*, disponibili in internet, dedicati proprio alla validazione dei siti ed alla verifica dei loro indirizzi (le *trace routes*, le stringhe di percorso che solo alcuni siti mostrano nella parte bassa del programma di navigazione). Accanto agli strumenti informatici progettati per assistere gli analisti, una serie di piccole accortezze possono conferire una sicurezza notevolmente maggiore al processo di identificazione delle informazioni importanti. Tra queste, la verifica dell'influenza che un sito internet ha a livello governativo o sui media, la verifica dell'uso di server propri in luogo di server altrui (servizio di solito a più basso costo quando non addirittura gratuito), il controllo, tramite strumenti leciti, del traffico che il sito produce, l'accertamento della frequenza di aggiornamento delle informazioni, l'analisi degli eventuali collegamenti con gruppi di pressione o movimenti di varia natura, della caratura dei siti collegati tramite ipertesti (*links*), delle informazioni che il sito fornisce su se stesso. Tra gli errori comuni, da segnalare l'eccessiva attenzione alla segretezza ed alla compartimentazione, i preconcetti, la mancanza di empatia (una dote essenziale che ogni analista deve possedere), l'eccessivo razionalismo, il conservatorismo o il cosiddetto *parrocchialismo*, ma anche l'etnocentrismo (mirror-imaging), il determinismo sia introspettivo (self-imaging) che rivolto ad eventi esterni (imaging) o la *Sindrome di Polianna* (wishful-thinking, eccessivo ottimismo).

La produzione di OSINT verte sull'utilizzo di quattro elementi fondamentali, nell'ordine costituiti da reports, tabulati di links informatici, istruzione a distanza e forum telematici di esperti. In relazione all'uso dei reports, emerge una netta differenza che contraddistingue l'OSINT da tutte le altre forme di intelligence, in cui questo tipo di strumenti costituisce il prodotto finale anziché una fonte intermedia. Un report può appartenere tanto alla categoria dell'OSIF quanto a quella dell'OSINT a seconda del grado di dettaglio posseduto, e può essere presentato sia in forma cartacea che elettronica. Molto importante, come già detto, è che il report rispetti una serie di standard formali relativi alla formattazione, impaginazione, metodo di inserimento o collegamento delle informazioni, predisposizione di un indice analitico dettagliato.

Tra le molte differenze che corrono tra un prodotto OSINT ed uno d'intelligence tradizionale, da citare è la possibilità che il report OSINT contenga documenti originali, cosa sostanzialmente impossibile nell'ambito dell'intelligence clandestina o basata su fonti protette. Ciò costituisce senza dubbio un vantaggio per gli analisti *all-source* e per coloro, come i comandanti, che in base alle informazioni ricevute devono prendere delle decisioni.

Le tavole di links informatici sono il prodotto intermedio dell'esplorazione avanzata di internet, mirante a scandagliare il cd. *deep web* alla ricerca di informazioni non reperibili attraverso i

migliori motori di ricerca, in grado di visualizzare al massimo il 15% delle informazioni disponibili, e neppure tramite l'utilizzo di appositi software in grado di consultare più motori di ricerca. Queste tavole sono semplici tabelle realizzabili con un qualsiasi word-processor, contenenti una valutazione dei links forniti ed un loro apprezzamento su base numerica.

L'istruzione a distanza è uno strumento di apprendimento "passivo" dal punto di vista dell'OSINT, il cui utilizzo è dovuto essenzialmente all'impossibilità che anche il più esperto degli analisti conosca tutte le materie che possono teoricamente rientrare nel suo campo d'azione. Se è vero che internet costituisce uno strumento prezioso, d'altra parte, è anche vero che il rendimento di chi lavora online tende ad essere molto più basso di chi non lo fa, a causa delle molte distrazioni che la rete genera e della mole di dati inutili che essa contiene. Per questo motivo, la NATO ha pianificato di creare un proprio servizio interno online di istruzione a distanza, sul modello dell'OSINT Centre predisposto dall'US Pacific Command.

I forum di esperti, organizzati su base interna, esterna oppure mista, sono lo strumento attraverso cui la NATO cerca di ottenere ulteriori intuizioni ed informazioni dalla comunità d'intelligence globale. Questi forum risiedono spesso su server di organizzazioni commerciali online che offrono adeguate garanzie di sicurezza ed affidabilità, e non sono dissimili da milioni di altri gruppi di discussione presenti nella rete. Ciò che veramente distingue questi forum da altri è l'esplicita sponsorizzazione da parte della NATO, mentre sono rare le restrizioni d'accesso che possono implicare la necessità di un invito esplicito. In generale, infatti, sebbene per la NATO sia importante conoscere i propri partners acquisendo sul loro conto alcuni dati in cambio della possibilità di condividere informazioni OSINT ai massimi livelli, l'accesso ai forum può avvenire anche in modo anonimo.

Tra i pregi che questo tipo di strumento possiede, una forte tendenza ad auto-organizzarsi senza che l'Alleanza debba provvedere a fornire stimoli o direttive particolari, ed una scalabilità e flessibilità senza pari, due fattori che contribuiscono ampiamente a compensare la necessità di copiare periodicamente l'intero contenuto dei forum, dovuta all'attuale impossibilità di applicare, su server altrui, filtri ed altri strumenti di screening dei dati ritenuti interessanti.

Diffusione

La differenza più sensibile tra l'OSINT e le altre discipline d'intelligence è il modo nel quale i prodotti finali possono essere custoditi e disseminati. L'OSINT, infatti, può essere condivisa con chiunque senza richiedere autorizzazioni politiche (Political Clearance) o di sicurezza, il che amplifica l'importanza di questo strumento soprattutto durante le operazioni *non-article V* in cui è della massima importanza mantenere e stimolare il dialogo con partners non-NATO e con le organizzazioni civili. I prodotti dell'OSINT possono essere condivisi in forma cartacea, essere riversati nella rete intranet NATO (WAN – Wide Area Network) e rese disponibili ad accessi esterni (*push-mode*) oppure trasmessi a destinatari particolari (*pull-mode, on demand*) sulla base della *policy* di volta in volta adottata. Il fatto che l'OSINT possa essere condivisa, infatti, non implica che tutti i suoi prodotti debbano necessariamente essere disseminati senza alcuna restrizione: si tratta di una decisione che viene presa in base ad un criterio utilitaristico, perché come tutte le altre attività NATO, l'OSINT ha come primo obiettivo quello di essere utile all'Alleanza.

L'utilizzo della WAN NATO implica la classificazione dell'informazione, ma presenta il pregio di assicurare un'ampia cornice di sicurezza alla circolazione dell'OSINT e di garantire l'accesso a tutto il personale NATO da ogni parte del mondo. Il principale svantaggio risiede proprio nella classificazione, ed in particolare nella necessità di separare l'informazione dalla fonte, a detrimento della possibilità di richiedere approfondimenti in modo intuitivo e di effettuare ulteriori controlli sull'affidabilità dell'autore.

Un sistema alternativo è costituito dai VPN (Virtual Private Networks), forum online il cui accesso è ristretto attraverso particolari procedure di sicurezza: in questo modo, l'OSINT può essere condivisa in modo integrale con un bacino di utenti conosciuti. D'altra parte, non tutti gli OSINT

Centres NATO hanno accesso al WAN dell'Alleanza, quindi è opportuno favorire l'utilizzo di sistemi più flessibili basati sul web. L'Alleanza sta già sperimentando il sistema VPN in collaborazione con l'US Open Source Information System (OSIS),²⁴ ed è probabile che nei prossimi anni il ricorso a questo strumento divenga sempre più massiccio.

Conclusioni

Il contesto internazionale in evoluzione impone a tutte le strutture impegnate nell'intelligence di adottare nuove soluzioni. La NATO, in particolare, sperimenta una crescente necessità di disporre di informazioni che i Paesi membri sono restii a fornire, soprattutto da quando la fine della guerra fredda, l'ingresso di nuovi Paesi membri ed associati ed il moltiplicarsi delle missioni fuori-area, hanno drasticamente trasformato il ruolo e le funzioni dell'Alleanza. In questo contesto, disporre di informazioni selezionate, non classificate e certe, costituisce un formidabile strumento non solo per stabilire una percezione comune all'interno della NATO, ma anche per costruire consenso e per dialogare efficacemente con un universo di organizzazioni civili in continua espansione. Accanto a ciò, la funzione d'intelligence, a tutti i livelli, si evolve progressivamente in direzioni che attribuiscono grande valore ai prodotti all-source, in relazione ai quali l'OSINT può fornire un valore aggiunto notevole: è stato notato che circa l'80% delle informazioni acquisite tramite l'intelligence tradizionale possono oggi essere ottenute sfruttando adeguatamente le fonti aperte²⁵, con risparmi enormi sia in termini economici che di tempo, e con grandi semplificazioni in materia di scoperta, trattamento e diffusione. L'OSINT può fornire notizie di contesto, punti di situazione, elementi tattici e molto altro, a patto che ad essa vengano adeguatamente adattati i criteri e metodi che l'intelligence ha sviluppato nella sua lunga storia e che le sia riconosciuto il rango non di pilastro, ma di elemento fondante della strategia d'intelligence del futuro. Il punto di vista della NATO è attualmente molto avanzato rispetto a quello di molti Paesi, ed in particolare di molti Stati europei, in cui il ricorso all'open source intelligence è concepito non come un elemento di base ma come uno strumento per colmare eventuali vuoti nei processi classificati²⁶. L'Alleanza, invece, disponendo peraltro di archivi classificati piuttosto ridotti e raramente posti oltre il livello tattico, confida molto in questo strumento, che in realtà non è affatto nuovo. Da sempre, infatti, gli Stati come gli individui fanno ricorso alle fonti aperte nel prendere le proprie decisioni²⁷, ma solo oggi a questi procedimenti si cerca di applicare un procedimento scientifico e sistematico. Durante la guerra fredda, ciò che oggi definiamo OSINT rientrava nei *collateral reports* della *single-source intelligence* e poteva contenere informazioni derivanti tanto da fonti aperte quanto da altri processi single-source, ma ad esso era attribuito un valore residuale²⁸ assolutamente non comparabile col ruolo fondativo, e di guida, che oggi è possibile affidare a questa fattispecie d'intelligence. Nell'ordine, sono quattro le funzioni che l'OSINT assolve direttamente in favore delle altre forme d'intelligence: completarla, indirizzarla, confermarne la validità, proteggerne le fonti ed i metodi. In via indiretta, l'OSINT conduce alla scoperta e catalogazione di fonti alternative utilizzabili dalle altre branche, favorisce la collaborazione di Paesi terzi, di popoli e persone, di organizzazioni specializzate. Da non dimenticare, infine, il fatto che le informazioni OSINT, grazie alle caratteristiche intrinseche possedute, nascono già ottimizzate per essere diffuse attraverso i virtual private network su cui l'Alleanza è disposta a scommettere per il futuro. La regola aurea in questo settore è infatti che più il livello di classificazione di un'informazione è basso più quest'ultima può essere diffusa; In una parola, se usata appropriatamente e se affiancata dalla connettività che la NATO si prefigge, l'OSINT è in grado di apportare un notevole contributo in direzione di quella flessibilità che costituisce l'obiettivo principale dell'Alleanza.

-
- ¹ Cfr. Jardines, E. A., "Understanding Open Sources" in *"Open Source Exploitation: A Guide For Intelligence Analysts"*, Joint Military Intelligence Training Center, Open Source Publishing Inc., in *NATO Open Source Intelligence Reader*, NATO SACLANT Intelligence Branch, Norfolk (VA), febbraio 2002, pg. 9.
- ² Cfr. *"NATO Open Source Intelligence Handbook"* NATO SACLANT Intelligence Branch, Norfolk (VA), novembre 2001, pg. V.
- ³ Può essere utile, per chi volesse approfondire l'argomento, visitare il sito internet <http://www.nato.int/intel>
- ⁴ Cfr. Friedman, R. S., "Open Source Intelligence", *Parameters*, Summer 1998, da Carlisle Army War College, in <http://www.carlisle.army.mil>
- ⁵ Opinioni severe nei confronti dell'open source intelligence sono state espresse in molti contesti. Per segnalare solo un contributo, è molto interessante l'articolo pubblicato su *Army Magazine* nel luglio 1997 da J. W. Davis: *"Open Source Information"*.
- ⁶ Cfr. anche Steele, R. D., "L'importanza dell'intelligence delle fonti aperte per il mondo militare", *Selezione Stampa*, luglio 1996, pg. 216. Tradotto dall'originale apparso su *Intelligence and Counterintelligence*, vol. 8, n° 4.
- ⁷ Cfr. *"NATO Open Source Intelligence Handbook"*, op. cit., pgg. 2-3.
- ⁸ A tale proposito, il NATO SACLANT ha prodotto nell'ottobre 2002 un apposito documento, il *"NATO Intelligence Exploitation of the Internet"*.
- ⁹ Qualche esempio, a questo proposito, è rinvenibile in. Zarca, P., "Le fonti aperte: uno strumento essenziale dell'attività di intelligence", *Per Aspera Ad Veritatem*, SISDE, n° 1, gen-apr 1995, pg. 237.
- ¹⁰ Vd. anche Steele, R. D., "L'importanza dell'intelligence delle fonti aperte per il mondo militare", op. cit., pg. 230.
- ¹¹ Cfr. Friedman, R. S., "Open Source Intelligence", op. cit., pg. 3.
- ¹² Cfr. *"NATO Open Source Intelligence Handbook"*, op. cit., pg. 7.
- ¹³ A questo proposito, si veda anche Dehqanzada, A., Florini, A. M., *"Secrets for Sale: How Commercial Satellite Imagery Will Change the World"*, Carnegie Endowment for International Peace, Washington D. C., 2000.
- ¹⁴ Cfr. Soule, M. H., Ryan, R. P., *"Grey Literature"*, Defense Technical Information Center, <http://www.dtic.mil>
- ¹⁵ A tale proposito, si veda Steele, R. D., "L'importanza dell'intelligence delle fonti aperte per il mondo militare", op. cit., pg. 223.
- ¹⁶ Ibidem, pgg. 218 e 220.
- ¹⁷ Ibidem, pg. 223.
- ¹⁸ Si veda, per qualche esempio, Turbeville Jr, G. H., Lt. Col. Prinslow, K. E., Lt. Col. Waller, R. E., "Assessing Emerging Threats Through Open Sources", *Military Review*, sett-ott 1999, pg. 72
- ¹⁹ Cfr. *"NATO Open Source Intelligence Handbook"*, op. cit., pg. 15.
- ²⁰ Vd. anche Steele, R. D., "L'importanza dell'intelligence delle fonti aperte per il mondo militare", op. cit., pg. 230.
- ²¹ Cfr. *"NATO Intelligence Exploitation of the Internet"*, NATO SACLANT Intelligence Branch, Norfolk (VA), ottobre 2002, pgg. 53 ss.
- ²² Su questo argomento, consultare anche "Managing Information Overload", *Jane's Intelligence Review*, marzo 2000, pgg. 50 ss.
- ²³ Ciò che gli americani definiscono *infotainment* per sottolineare la confluenza tra informazione ed intrattenimento.
- ²⁴ Informazioni approfondite sull'OSIS sono contenute in Turbeville Jr, G. H., Lt. Col. Prinslow, K. E., Lt. Col. Waller, R. E., "Assessing Emerging Threats Through Open Sources", op. cit., pgg. 70 ss.
- ²⁵ Cfr. Adm. Studeman, W., "Teaching the giant to dance: contradictions and opportunities in open source within the intelligence community", *American Intelligence Journal*, Spring-Summer 1993, pgg. 11 ss.
- ²⁶ Cfr. Zarca, P., "Le fonti aperte: uno strumento essenziale dell'attività di intelligence", op. cit, pg. 238.
- ²⁷ Cfr. Friedman, R. S., "Open Source Intelligence", op. cit.
- ²⁸ Cfr. *"NATO Open Source Intelligence Handbook"*, op. cit., pg. 39. Vd. anche Turbeville Jr, G. H., Lt. Col. Prinslow, K. E., Lt. Col. Waller, R. E., "Assessing Emerging Threats Through Open Sources", op. cit., pg. 71.