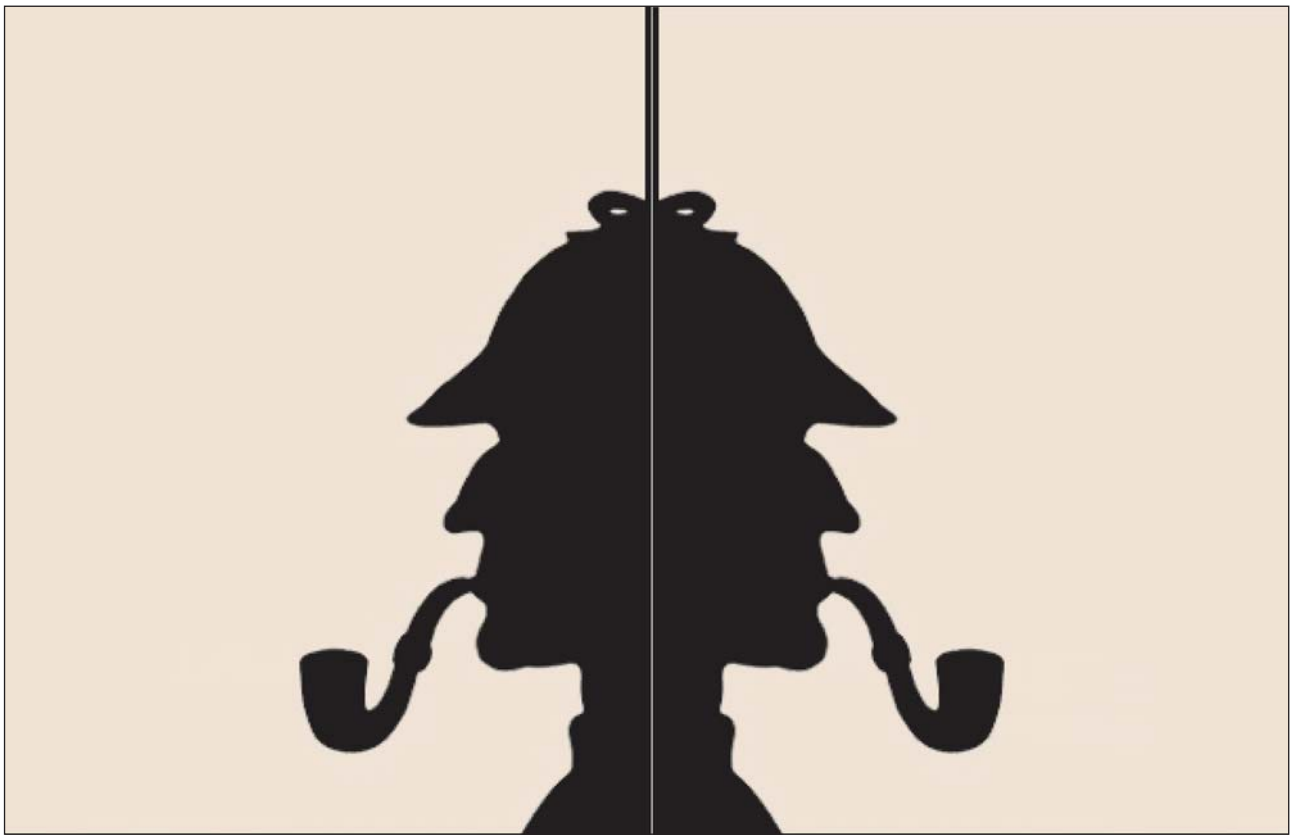
Open Source Intelligence

Dott. Carlo Centoducati
Master in Studi Internazionali Strategico-Militari

Cenni sulla dottrina alleata



Gli ultimi due decenni sono stati caratterizzati da mutamenti epocali come la profonda trasformazione degli assetti geopolitici e strategici globali o la nuova compressione delle distanze generata dal progresso tecnologico. L'inedita dimensione unipolare degli equilibri internazionali, l'assenza di un ordine mondiale stabile, la proliferazione di armi nucleari, i conflitti etnico-religiosi ed il nuovo terrorismo internazionale determinano, in questo contesto, una progressiva revisione dei concetti di Difesa e di sicurezza.

Nel frattempo, la diffusione dell'accesso ad internet ha mutato il mondo dell'informazione e della conoscenza contribuendo, assieme ad altri fenomeni, alla formazione di una cultura globale e di molte culture ad essa antagoniste e determinando nuove forme di integrazione e di contrapposizione tra individui e tra organizzazioni.

Nell'accelerazione generalizzata che caratterizza il nostro tempo, alcuni elementi storicamente di secondo piano vengono riscoperti. Soprattutto nei Paesi nordeuropei ed anglosassoni, l'*intelligence* e le sue possibili evoluzioni, con particolare attenzione alle fonti aperte, (OSINT/OSI – *Open Source Intelligence*) torna sotto i riflettori.

L'*Open Source Intelligence*

Non è ancora disponibile una definizione

condivisa di questa forma di *intelligence* (1). In ambito NATO, l'OSINT consiste nella raccolta, selezione, distillazione e diffusione di informazioni non classificate ad una comunità ristretta ed in relazione a specifici argomenti (2). Non si tratta ovviamente di ricerca accademica, economica o giornalistica, nella misura in cui non si acquisisce o genera conoscenza, ma si fa uso di strumenti d'*intelligence* applicati ad una più ampia tipologia di fonti. Nell'ambito di una organizzazione come la NATO, ciò risulta particolarmente utile per consentire a tutte le componenti nazionali di condividere informazioni relative all'area delle operazioni (*Area of Operations*), ma anche per dialogare in modo efficace con le organizzazioni civili. Il dibattito su questi fattori è ampio e vivace (3), anche in relazione ai sistemi per consentire un miglior accesso alle informazioni riducendo le richieste di autorizzazioni specifiche. D'altra parte, la NATO si integra divenendo un *sistema*, laddove il terrorismo globale rende i sistemi-Paese più vulnerabili e quindi più integrati, esigendo che comparti una volta estranei dialoghino tra loro determinando strutture della Difesa e della sicurezza sempre più dinamiche, disperse e collaborative (4). Il dialogo è tuttavia un elemento problematico nel settore dell'*intelligence*, ove scambiare informazioni classificate collide con il bisogno di proteggere i propri interessi, le proprie procedure e le proprie fonti (5). Non è difficile, dunque, comprendere quanto la NATO sia stata danneggiata dall'impossibilità di predisporre strumenti sistematici di circolazione delle informazioni. Si tratta di una situazione destinata a cambiare, ma occorre contemperare l'ampio bisogno di comunicazione con la protezione delle informazioni sensibili. L'*intelligence* delle fonti aperte sembra costituire una risposta a questa esigenza (6), a patto che ad essa siano applicati i metodi di trattamento delle informazioni dell'*intelligence* tradizionale. Il fine è quello di alimentare al meglio l'assemblaggio di prodotti cd. *all-source intelligence*, ed è necessario accostarsi all'OSINT come ad una disciplina scientifica.

In questo senso, almeno quattro elementi devono essere considerati: le definizioni, le fonti, la direzione ed il ciclo dell'OSINT.

Definizioni

L'*open source intelligence* non costituisce un processo, ma un prodotto. Esiste infatti una gerarchia tra dati da fonti aperte (*Open Source Data* (OSD): documenti interni, registrazioni audio-video, immagini, *debriefing* ed altre fonti primarie), informazioni da fonti aperte (*Open Source Informations*: dati grezzi secondari emersi nel processo di analisi delle OSD, di solito disponibili nella forma di *report* specialistici, quotidiani, libri), *intelligence delle fonti aperte* (OSINT: informazioni derivanti da un processo volontario di scoperta, selezione, distillazione e distribuzione ad un pubblico selezionato) ed OSINT verificate (OSINT-V: il prodotto finale destinato al confronto con informazioni classificate) (7) cui può essere attribuito il più alto livello di aderenza alla realtà.

Le fonti dell'OSINT

Il sistema di fonti relativo all'OSINT è composto da dati accessibili legalmente attingendo dal mondo pubblico e privato sia in modo gratuito che a pagamento. Indubbiamente, internet è una preziosa risorsa (8), ma non l'unica né necessariamente la migliore. Tra i milioni di informazioni disponibili *online*, infatti, solo alcune sono realmente utili e la loro identificazione non è affatto semplice: gli analisti si confrontano quotidianamente con l'impossibilità di leggere, controllare e verificare tutte le informazioni, identificarne l'autore, la data e l'ora, stabilire il grado di imparzialità della fonte ed i suoi obiettivi (9), e vi sono

(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

difficoltà nel comprendere informazioni in varie lingue, formattarle adeguatamente, navigare nella rete in modo anonimo per sfuggire ad operazioni di contro-*intelligence* (*deception* - inganno) (10).

Oltre ad internet, il mondo dell'OSINT comprende fonti più "tradizionali" tra le quali un posto di rilievo spetta ai servizi d'*intelligence* forniti da organizzazioni private, alcune delle quali (si pensi a *Lexis-Nexis, Independent Information Brokers, Dialog, Rand, Jane's* ed altri) (11) operano da decenni selezionando, verificando, formattando, indicizzando, riassumendo e presentando informazioni rilevanti, anche *online*.

Un'altra tipologia di fonti è quella della "letteratura grigia" (*Grey Literature*), costituita da informazioni ottenibili solo attraverso il contatto diretto o l'uso di canali particolari (12). Si tratta di materiale non pubblicato né catalogato se non in ambienti ristretti, che include documenti interni e *reports* tecnici di amministrazioni, sindacati, ONG ed altri soggetti. Cresce inoltre il peso delle immagini commerciali satellitari che stanno rivoluzionando l'*Imagery Intelligence* (13) (IMINT) grazie all'alto livello di dettaglio, ai costi accessibili e ad una cornice giuridica internazionale piuttosto permissiva.

L'*intelligence* umana (HUMINT – *Human Intelligence*) è sostituita in questo settore dal ricorso a persone che hanno un'esperienza diretta del campo o evento di interesse (*Overt Human Observers*), (14) utili soprattutto in relazione a circostanze o luoghi (si pensi ad alcuni Paesi africani) su cui non è facile ottenere informazioni (15), o agli esperti (*Overt Human Experts*) (16), il cui contributo può essere richiesto presso università, centri studi, organizzazioni governative e non, anche *online*. Passando ai soggetti dai quali è possibile attingere informazioni, i servizi di sicurezza nazionali, pur non essendo direttamente coinvolti nel soddisfacimento dei requisiti OSINT, possono alimentarne il processo tramite informazioni non classificate. Stati Uniti, Olanda, Danimarca, Norvegia e Gran Bretagna (ma altri Stati dispongono di capacità minori in crescita) sono molto abili in questo campo, disponendo di cellule OSINT ben integrate nella struttura nazionale di *all-source intelligence*.

Anche le Ambasciate e le missioni diplomatiche costituiscono una buona fonte di OSINT a basso costo. Si tratta di istituzioni estranee ai processi OSINT, ma un certo livello di coordinamento, anche informale, è suscettibile di produrre ripercussioni positive e di ampia scala.

Da non dimenticare, inoltre, le Camere del Commercio, molto diffuse e ritrovo di comunità specializzate ed informate su argomenti di scala anche non nazionale, molto utili soprattutto nelle aree in cui i contingenti vengono dispiegati sul terreno.

Menzione particolare va infine riservata alle organizzazioni internazionali, non governative e religiose, la cui diffusione ha raggiunto livelli di capillarità elevati. Le agenzie delle Nazioni Unite, il Comitato Internazionale della Croce Rossa, Medici Senza Frontiere, l'Opus Dei, l'Islamic World Foundation ed altre organizzazioni sperimentano quotidianamente il contatto con realtà locali variegate, disponendo di informazioni il cui accesso è spesso difficoltoso.

La direzione

Come è noto, in ambito NATO al Comandante spettano sia la definizione dei requisiti essenziali di informazione (EEI - *Essential Elements of Information*) che la costituzione degli assetti *intelligence*. In questo contesto, l'OSINT non è necessariamente un servizio fornito su base nazionale, né un elemento dalla rigida collocazione: se la cellula OSINT è subordinata alla cellula *intelligence* (CJ2 – *Combined Joint Intelligence Cell*), è evidente che elementi come il comandante della cooperazione civile-militare (CIMIC), gli addetti alla pubblica informazione o la Polizia Militare possono costituire un consiglio informale di grande efficacia. I comandanti ed i loro staff dovrebbero inoltre articolare in modo puntuale le proprie richieste. Non è infrequente, infatti, che le Richieste di Informazioni (RFI - *Requests for Information*) siano ampie o che vengano richiesti vaghi punti di situazione. Attraverso le fonti aperte possono essere soddisfatti tanto i bisogni generici quanto quelli specifici,(17) a patto che le linee guida fornite dall'alto siano accuratamente specificate.

(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. Soule, M. H., Ryan, R. P., "*Grey Literature*", Defense Technical Information Center, http://www.dtic.mil
(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) A tale proposito, si veda Steele, R. D., "*L'importanza dell'intelligence delle fonti aperte per il mondo militare*", op. cit., pg. 223
(15) Ibidem, pgg. 218 e 220
(16) Ibidem, pg. 223
(17) 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

La pianificazione e la conduzione delle operazioni militari, infine, sono processi ciclici nei quali è fondamentale una comunicazione bi-direzionale, o in altri termini, un costante dialogo tra fornitori ed utilizzatori delle informazioni.

Il ciclo dell'*intelligence* applicato alle fonti aperte

Poiché il bisogno di informazioni da parte della NATO è ampio, destinato a crescere e dipendente tanto dalle missioni che da condizioni geopolitiche mutevoli, non è possibile pensare alla creazione di un database informativo permanente. L'attenzione deve essere dunque riposta non tanto sulle informazioni quanto sulle fonti e sui metodi, al fine di costruire rapidamente, ed in modo efficiente, processi flessibili di produzione OSINT.

Il ciclo dell'*intelligence* si compone di quattro fasi principali (le "four Ds": *discovery, discrimination, distillation and dissemination* (18)) suddivise in sottofasi a costituire un unico sistema. 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* preordinati. Il processo è molto articolato e spesso mutevole e, diversamente da quanto avviene per altre forme d'*intelligence,* la dottrina OSINT NATO è tuttora in fase di formazione, per cui una certa flessibilità al suo interno 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, nelle varie fasi, risultano di particolare interesse.

Scoperta: selezione ed interrogazione delle fonti

Il primo passo nella costituzione di solide capacità OSINT è la creazione di un sistema di fonti integrato ed efficiente. Conoscere gli esperti e poter accedere ai loro lavori sono requisiti essenziali che l'Alleanza ha voluto soddisfare predisponendo un inventario di esperti (SMEI - *Subject-Matter Experts Inventory*) sia presso i singoli comandi che a livello centralizzato, e grande attenzione viene riservata alle Camere di Commercio, agli istituti di ricerca, alle università, organizzazioni professionali e non governative. L'analisi OSINT deve inoltre fare i conti con i limiti legati alla sicurezza delle operazioni (OPSEC – *Operation Security*), requisito che può essere soddisfatto sia tramite l'uso di intermediari (19) che attraverso procedure di anonimizzazione della navigazione internet (20). Inoltre, facendo l'OSINT ampio ricorso al contributo di organizzazioni esterne, l'OPSEC può essere garantita attraverso la stipula di accordi di segretezza (NDA – *Non-Disclosure Agreements*) protetti da clausole economiche. La collaborazione con agenti privati implica anche numerosi vincoli legati alle normative sul *copyright* che alcuni Governi escludono per legge riducendo l'interesse che gli operatori hanno a fornire prodotti di qualità. Quello del rispetto del *copyright*, secondo la dottrina NATO, è invece un presupposto irrinunciabile al fine di mantenere il più alto livello di flessibilità e di efficacia possibile, anche a costi maggiori.

La NATO sperimenta anche molti problemi di natura linguistica soddisfatti sia a livello nazionale che dall'Alleanza, anche a livello di singolo contingente. A questa pratica è legata l'esigenza di attribuire agli esperti adeguate certificazioni di sicurezza (*Security Clearances*). I servizi nazionali, d'altra parte, sono raramente disposti a distogliere prezioso *know-how* concedendolo alla NATO, alimentandone le difficoltà nel reperimento di interpreti e traduttori di qualità.

Il processo di adeguamento della NATO a queste nuove esigenze è parte integrante del *Future Intelligence Architecture Plan* dell'Organizzazione. Il meccanismo è infatti lontano dal funzionare adeguatamente: 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 questo ed i propri database classificati, e la stessa comunicazione con l'esterno, irrinunciabile per l'OSINT, è talvolta fonte di problemi sia a causa di semplici difficoltà burocratiche, sia per ristrettezze finanziarie, sia infine per l'esistenza, in alcuni Paesi, di norme che ostacolano il contatto tra personale *intelligence* ed esperti privati.

Strategie di discriminazione

Il cuore dell'*intelligence* è senza dubbio la selezione delle informazioni. In ambito NATO spetta allo *staff intelligence* di stabilire a quali domande è possibile rispondere e quali debbano essere "girate" ad altri atto-

(18) Cfr. "*NATO Open Source Intelligence Handbook*", op. cit., pg. 15
(19) Vd. anche Steele, R. D., "*L'importanza dell'intelligence delle fonti aperte per il mondo militare*", op. cit., pg. 230
(20) Cfr. "*NATO Intelligence Exploitation of the Internet*", NATO SACLANT *Intelligence Branch, Norfolk* (VA), ottobre 2002, pgg. 53 ss.

ri tramite RFI. La raccolta delle informazioni è il risultato tipico della traduzione di una RFI in uno sforzo dell'*intelligence* tradizionale, mentre in ambito OSINT lo sforzo principale è sempre diretto alla selezione ed all'integrazione. Esistono, in questo senso, almeno tre strategie applicabili, ciascuna adatta a specifici contesti: *analyst-driven* (fondata sulle capacità dell'analista di discernere gli elementi utili), *events-driven* (uno sforzo più accentuato e concentrato nel tempo), e *scheduled* (adatta ad attività di aggiornamento periodico). Quando si effettua un'analisi il tempo e le informazioni disponibili sono i fattori di maggior rilievo ma anche due elementi facilmente in conflitto tra loro. Il rischio, in tema di OSINT, consiste nel sacrificare troppo tempo nella validazione delle fonti a scapito dell'analisi e del livello di dettaglio (21). Una parte di questo problema può essere risolta predisponendo un elenco aggiornato e verificato delle fonti, l'altra va curata con la formazione.

Strumenti di distillazione

La fase critica del ciclo dell'OSINT consiste nella distillazione delle informazioni. Lavorare con le fonti aperte nasconde infatti mille insidie, ed è frequente che gli operatori commettano degli errori oppure siano vittime di inganni. D'altra parte, anche attribuire un valore d'*intelligence* ad informazioni ottenute da servizi informativi nazionali è una pratica sconsigliata ma diffusa. In questi casi, tuttavia, gli analisti hanno a disposizione il proprio *background* professionale ed una certa conoscenza della fonte e dei suoi possibili interessi, cosa non semplice in relazione alle *open sources* sulle cui fonti le informazioni sono spesso carenti.

L'informazione, inoltre, tende spesso ad essere improntata al sensazionalismo (22) e gli stessi processi d'*intelligence* talvolta scricchiolano sotto il peso della produzione di consenso. È dunque necessario che gli operatori mantengano un alto livello di vigilanza, al fine di evitare perlomeno gli errori più comuni. Questi vanno dall'errata formattazione dell'informazione all'assenza di dati come la data o la fonte, o ancora alla mancata verifica della sua credibilità. Tra gli errori più gravi, da segnalare l'eccessiva attenzione alla segretezza, la compartimentazione, i preconcetti, la mancanza di empatia, l'eccessivo razionalismo, il conservatorismo ed il *parrocchialismo*, ma anche l'etnocentrismo (*mirror-imaging*), le forme di determinismo (*imaging* e *self-imaging*) o la *Sindrome di Polianna* (*wishful-thinking*, eccessivo ottimismo).

L'allora NATO-SACLANT (oggi *Allied Command Transformation*) ha elaborato per i propri analisti una serie di linee guida destinate a fornire strumenti per la verifica del contenuto dei siti internet. Di particolare interesse risultano i molti *tools* gratuiti dedicati alla validazione dei siti e degli indirizzi (le *trace routes*). Accanto a questi strumenti, una serie di piccole accortezze come la verifica dell'influenza che un sito ha a livello governativo o sui *media*, il controllo del traffico, della frequenza di aggiornamento, dei collegamenti con gruppi o movimenti, del tipo di siti collegati, delle informazioni che il sito fornisce su se stesso, dell'uso di server proprietari o altrui (servizio spesso gratuito) possono amplificare notevolmente la sicurezza del processo. Gli strumenti fondamentali dell'OSINT sono i *reports*, i tabulati di *links* informatici, l'istruzione a distanza ed i *forum* telematici.

In relazione ai *reports*, emerge una netta differenza con le altre forme di *intelligence* in cui questi costituiscono il prodotto finale anziché una fonte intermedia. Un *report* OSINT può contenere documenti originali, cosa insolita nell'*intelligence* clandestina, può appartenere all'OSIF o all'OSINT a seconda del grado di dettaglio e può essere presentato sia in forma cartacea che elettronica purché rispetti i requisiti di formattazione, a tutto vantaggio degli analisti *all-source* e degli organi decisionali.

Le tavole di *links* informatici sono il prodotto dell'esplorazione del cd. *deep web* alla ricerca di informazioni non reperibili attraverso i motori di ricerca (in grado di visualizzare al massimo il 15% delle informazioni disponibili). Queste tavole sono semplici tabelle di *word-processor* contenenti una valutazione dei *links* forniti ed un loro apprezzamento su base numerica.

Poiché nessun analista è onnisciente, l'istruzione a distanza è uno strumento di apprendimento "passivo" il cui utilizzo è fortemente consigliato dalla NATO nell'ambito dell'OSINT. Se infatti internet costituisce uno strumento prezioso, è anche vero che il rendimento di chi lavora *online* tende ad essere più basso a causa della mole di dati inutili che internet contiene. Per questo motivo, la NATO ha pianificato di creare un proprio servizio *online* di istruzione a distanza, sul modello dell'*OSINT Centre* dell'*US Pacific Command*.

I *forum* di esperti sono lo strumento attraverso cui la NATO si avvale del contributo dalla comunità d'*in-*

(21) Su questo argomento, consultare anche "Managing Information Overload", *Jane's Intelligence Review*, marzo 2000, pgg. 50 ss.

(22) A questo proposito, il noto esperto di *Open Source Intelligence* Alessandro Politi parlerebbe di *info-tainment* per sottolineare la confluenza tra informazione ed intrattenimento. Alessandro Politi, intervento al Centro Alti Studi per la Difesa, Roma, 6 aprile 2005

telligence globale. Come molti altri gruppi di discussione *online*, questi forum risiedono spesso su server di organizzazioni che offrono adeguate garanzie di sicurezza. Il vero elemento di distinzione è l'esplicita sponsorizzazione da parte della NATO, e sono rare le restrizioni d'accesso. In generale, infatti, sebbene per la NATO sia importante conoscere i propri *partner*, l'accesso ai forum è consentito anche in modo anonimo. Tra i pregi che questo tipo di strumento possiede, una forte tendenza ad auto-organizzarsi ed una scalabilità e flessibilità senza pari, che contribuiscono a compensare la necessità di copiare periodicamente l'intero contenuto dei forum, dovuta all'impossibilità di applicare, su server altrui, strumenti di *screening* dei dati interessanti.

Modalità di diffusione

La differenza più sensibile tra l'OSINT e le altre discipline d'*intelligence* sta nel modo in cui i prodotti finali possono essere disseminati. L'OSINT, infatti, può essere condivisa senza richiedere autorizzazioni politiche o di sicurezza, semplificando ad esempio le operazioni *non-article V* in cui il dialogo con *partner* non-NATO o civili è della massima importanza. I prodotti OSINT possono essere condivisi in forma cartacea o essere riversati nella *Wide Area Network* (WAN) NATO per accessi continui (*push-mode*) oppure condizionati (*pull-mode*, *on demand*) sulla base della *policy* adottata. Il fatto che i prodotti OSINT possano essere condivisi, infatti, non implica che essi debbano esserlo: si tratta di decisioni che rispondono ad un criterio utilitaristico.

L'utilizzo della WAN NATO impone la classificazione dell'informazione. Ciò assicura una cornice di sicurezza e garantisce l'accesso a tutto il personale NATO nel mondo, ma richiede di separare l'informazione dalla fonte a detrimento della possibilità di effettuare approfondimenti e di controllare l'affidabilità dell'autore. Un sistema alternativo è costituito dai VPN (*Virtual Private Networks*), *forum online* il cui accesso è ristretto affinchè l'OSINT possa essere condivisa con un bacino di utenti conosciuti. D'altra parte, poiché non tutti gli *OSINT Centres NATO* hanno accesso alla WAN, questo sistema assicura una flessibilità maggiore (23).

L'attuale contesto internazionale impone alle strutture di *intelligence* di adottare nuove soluzioni. La NATO, in particolare, sperimenta una crescente necessità di informazioni che i Paesi membri sono restii a fornire, soprattutto da quando il ruolo e le funzioni dell'Alleanza si sono radicalmente modificati. In queste condizioni, disporre di informazioni sensibili, non classificate ma certe, costituisce un imperativo. Accanto a ciò, la funzione d'*intelligence* si evolve attribuendo grande importanza ai prodotti *all-source* cui l'OSINT può contribuire fino all'80% (24) determinando enormi risparmi. L'OSINT può fornire notizie di contesto, elementi tattici e molto altro, a patto che ad essa venga riconosciuto il rango di elemento fondante della strategia d'*intelligence* del futuro. Il punto di vista della NATO è molto avanzato rispetto a quello di molti Stati, soprattutto europei, in cui il ricorso all'*open source intelligence* è concepito come residuale (25). L'Alleanza, invece, disponendo peraltro di archivi classificati raramente posti oltre il livello tattico, confida molto in questo strumento, che in realtà non è affatto nuovo (26) ma solo oggi scientificamente riconsiderato.

Nell'ordine, sono quattro le funzioni che l'OSINT assolve direttamente in favore delle altre forme d'*intelligence*: completarle, indirizzarle, confermarne la validità, proteggerne le fonti ed i metodi. In via indiretta, l'OSINT conduce alla scoperta di fonti alternative, 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 loro caratteristiche, nascono già ottimizzate per essere diffuse attraverso i VPN su cui l'Alleanza sta scommettendo. La regola è infatti che più basso è il livello di classificazione più un'informazione 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. ■

(23) L'Alleanza sta già sperimentando il sistema VPN in collaborazione on l'*US Open Source Information System* (OSIS), ed è probabile che nei prossimi anni il ricorso a questo strumento divenga sempre più massiccio. 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.

(24) 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.

(25) Cfr. Zarca, P., "*Le fonti aperte: uno strumento essenziale dell'attività di intelligence*", op. cit, pg. 238

(26) Cfr. Friedman, R. S., "*Open Source Intelligence*", op. cit. 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, ma ad esso era attribuito solo un valore di contesto. Cfr. anche "*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