

Intelligence Mining 2.0

Inviato da Giovanni Nacci
 giovedì 28 agosto 2008
 Ultimo aggiornamento lunedì 29 settembre 2008

Di tanto in tanto, negli ambienti in qualche modo vicini a quelli della "Intelligence Community", riprende vigore il dibattito circa la validità (sia in senso strategico che in senso tattico-operativo) - dei metodi, dei sistemi e delle tecnologie per l'Intelligence da Fonti Aperte e sul ruolo che l'OSINT ha, o potrà avere, all'interno del "Macro-sistema di Sicurezza".¹ (qui la versione PDF)

Il punto centrale della questione sembra essere quello di valutare quanto ed in che modo l'OSINT sia realmente funzionale² al complesso processo di costruzione del cosiddetto "prodotto di intelligence".

I pareri che abbiamo avuto modo di rilevare sono concordi nel considerare l'OSINT come uno strumento di impiego universale, la cui peculiare predilezione per le "fonti aperte" lo rende maggiormente adatto alla analisi strategica intesa in senso ampio, finalizzata alla definizione di linee di indirizzo generali. D'altro canto, è abbastanza diffusa l'idea che l'OSINT non dimostri la stessa utilità in contesti maggiormente caratterizzati da aspetti tattici ed operativi o comunque nelle attività analitiche che si basano su informazioni classificate. Riguardo quest'ultima considerazione crediamo possa esistere una differente chiave di lettura che vogliamo in questa sede approfondire. Sebbene per "fonte aperta" si possa intendere quella fonte che "...è fin dal principio esplicitamente finalizzata alla sua comunicazione (e/o scambio) anche a prescindere dall'eventuale costo o valore economico di mercato della stessa..."³ è pur vero che il soggetto che è titolare di un determinata informazione, per quanto classificata, vi accede liberamente come se fosse - appunto - fonte aperta⁴. Ne è la riprova la banale (ma neanche poi tanto) considerazione che le misure poste a limitazione della disponibilità di una informazione valgono (a seconda del livello di qualifica apposto) nei confronti di terzi soggetti e mai del medesimo soggetto che appone la qualifica. Se così non fosse il soggetto - una volta qualificata l'informazione come indisponibile anche a se stesso - rinuncerebbe di fatto al possesso di quella informazione, cui in ogni caso non potrebbe più accedere, nemmeno per una eventuale declassifica⁵.

E' ovviamente un paradosso, ma è un paradosso sul quale conviene soffermarsi per dire che l'informazione da "fonte aperta" è anche - forse soprattutto e, aggiungiamo, prima di ogni altra cosa - tutta l'informazione (più o meno classificata) che possediamo già. Uno dei più famosi "assiomi" della teoria dell'OSINT - quello che esplicita il tipico "sbilanciamento sulle fonti" dell'Open Source Intelligence - recita che è indispensabile "conoscere chi conosce". Ne consegue che:

- avere la disponibilità dell'accesso alle fonti (cioè del "chi conosce") è ancora più importante che accumulare informazioni;

- tra tutte le fonti, la fonte primaria è la propria conoscenza;

- l'Osint è prioritariamente un intelligence di fonti e solo successivamente un intelligence di informazioni. Pertanto la prima attività analitica di un procedimento di intelligence (in qualsiasi contesto) consiste nella attenta valutazione della conoscenza endògena. Infatti solo valutando con esattezza ciò che sicuramente sappiamo già è possibile prevedere "ciò che dovremmo sapere" e che ancora non conosciamo. Dunque se l'intelligence da fonte classificata è per definizione un strumento a supporto delle attività decisionali dei decisori, l'intelligence da fonti aperte ne rappresenta un concetto sovraordinato, proprio perché è definito dell'unione di due insiemi:

- quello composto da tutte le fonti/informazioni esterne esistenti e potenzialmente disponibili (ma del quale non conosciamo la cardinalità⁷);
- quello delle fonti/informazioni interne che possediamo già e che sono certe, enumerabili e ci si passi il termine, disponibili - "aperte" - per default. Riassumendo, e senza addentrarci troppo nella teoria della validazione delle fonti, possiamo senza dubbio affermare che il concetto di disponibilità⁸ di una fonte/informazione va scisso - rispettivamente - in due diverse accezioni:
 - il concetto di disponibilità universale, che riguarda le fonti/informazioni indirettamente e potenzialmente acquisibili dalla maggior parte degli individui;
 - quello di disponibilità particolare, che concerne le fonti/informazioni già direttamente ed effettivamente disponibili. Sulla base di quanto detto, ci sembra evidente che i metodi, i sistemi e le tecnologie di Osint rimangono validi ed utilmente applicabili anche sulla conoscenza classificata di una Organizzazione, incardinandosi anzi come core application all'interno del processo di intelligence convenzionale. La base di conoscenza detenuta da una Agenzia⁹ non è cosa diversa da quella che in altri campi chiamiamo "conoscenza aziendale": un repository di informazioni più o meno rilevanti, più o meno organizzate, più o meno strutturate, rinvenibili all'interno della struttura organizzativa. Per una Agenzia - ancor di più che per qualsiasi azienda, per quanto di grandi dimensioni¹⁰ - la conoscenza aziendale è lo strumento di gestione strategica, finalizzata al raggiungimento di una concreta condizione di vantaggio competitivo. I problemi sorgono quando l'estensione e la complessità di questa base di conoscenza supera un certo limite fisiologico (diverso a seconda dei casi) oltre il quale - se tale conoscenza rimane unmanaged - il rischio è quello di perdere la consapevolezza di "ciò che si sa" e di ciò che, al contrario, "non si sa", varcando quella pericolosa (anche perché difficilmente identificabile) soglia che dalla conoscenza conduce alla "illusione della

conoscenza”11. Un deficit di consapevolezza (o di fiducia12) nelle prestazioni della propria base di conoscenza, porta – nel migliore dei casi - ad una analisi inefficiente: l'operatore rischia ad incaponirsi nel cercare altrove qualcosa che invece è già disponibile all'interno (ma non lo si sa, o non lo si crede) o viceversa, con immaginabile dispendio di risorse. In tutte le organizzazioni, così come nelle Agenzie, accade che con il tempo la conoscenza si estenda senza che operatori, funzionari e dirigenti se ne rendano realmente conto. Quantità ingenti di dati elementari, informazioni più o meno complesse, documenti, cartelle, file si accumulano disordinatamente formando un groviglio informativo pressoché impossibile da districare. La maggior parte dei moderni sistemi informativi aziendali (anche quando dotati di algoritmi di categorizzazione e classificazione basati su set di keyword) dati omogenei o quantomeno formalizzati in modo rigidamente strutturato. Il problema sorge quando capita di dover reagire di fronte ad una evoluzione architetturale della conoscenza che, se vogliamo, è ciò che a noi interessa di più13. lavorano bene anche con grandi quantità di dati, ma devono essere Un'altra importante fetta di conoscenza aziendale è “imprigionata” all'interno di una quantità inaspettatamente grande di documenti testuali redatti in in linguaggio naturale14 conservati da operatori, dipendenti, funzionari su risorse periferiche del sistema informativo (PC portatili, DVD e CD-Rom, chiavette USB, schede di memoria per cellulari, smart phone, eccetera). Appunti, note, rapporti non ufficializzati o mai inoltrati, bozze di studi, analisi iniziate e poi abbandonate, archivi di e-mail, agende, calendari eccetera: tutta questa conoscenza latente rappresenta una unica grande “fonte aperta” endogena alla organizzazione, che rischia di venire sistematicamente ignorata dal processo di intelligence e che invece è necessario prendere in considerazione, se non altro per motivi di sicurezza. I metodi, i sistemi e le tecnologie15 di cui l'OSINT si serve, quando applicati alla conoscenza interna delle organizzazioni, permettono di ottenere (in tempo pressoché reale) una visione dinamica della conoscenza disponibile, evidenziando – anche grazie al supporto interattivo di una interfaccia grafica complessa – informazioni, significati, concetti e tutte le relazioni fra essi intercorrenti, relazioni che prima erano latenti o che - per molti motivi - erano passate inosservate, magari oscurate da relazioni meno rilevanti ma più evidenti. In questo senso l'OSINT non è più solo una attività di intelligence rivolta all'esterno, ma diventa anche un processo analitico introspettivo16 che - per endogenesi – da un lato approfondisce la comprensione della propria knowledge base e dall'altro favorisce la qualità dell'intero processo di realizzazione del “prodotto di intelligence”. In termini aziendali potremmo definirla come una “funzione di controllo interno”, specificatamente demandata alla osservazione dello “stato di salute” e delle prestazioni della conoscenza aziendale. Una simile attività, che potremmo chiamare “Introspective Intelligence Mining”17, a nostro parere dovrebbe essere la principale tra le preoccupazioni di una Agenzia, anche in considerazione del fatto che la maggior parte dei recenti “fallimenti” attribuiti (o attribuibili) all'“intelligence” sembrano proprio scaturire da una mancata o insufficiente percezione18 di conoscenze che erano già a disposizione dell'Intelligence Community e non - o quantomeno non solo - di altre che avrebbero potuto essere potenzialmente acquisite. In conclusione, non crediamo che intelligence classificata e intelligence da fonte aperta siano concetti in antitesi. Né che siano due facce di una stessa medaglia destinate a non incontrarsi mai. Così come è anche da sfatare il mito che l'intelligence classificata sia un affare esclusivo dei “Servizi” mentre quella da fonti aperte sia una pseudo-intelligence alla portata di tutti. La particolarità che più caratterizza l'Osint – come disciplina - rispetto all'intelligence classificata, sta nel fatto di essersi dovuta costruire, fin dall'inizio, tutti gli strumenti analitici necessari per astrarre concetti omogenei a partire da quantità vastissime di dati e informazioni assolutamente eterogenee. Ciò è stato possibile attingendo ed integrando secondo le necessità le migliori conoscenze disponibili in una vasta gamma di discipline tra le quali la matematica, la statistica, la linguistica, l'informatica, tanto che non è poi così bizzarro sostenere che la formalizzazione stessa della teoria dell'Open Source Intelligence sia stata, di per sé, il frutto di una attività di Open Source Intelligence. Forse i tempi sono maturi per cominciare a pensare ad una riformulazione di quella che ci piace chiamare l'“ontologia dell'intelligence” superando barriere culturali e idee preconcepite. Questa nostra società è caratterizzata da equilibri sempre più complessi, articolati, in continua e repentina evoluzione che sono - proprio per questo motivo - più fragili. E' lecito aspettarsi che la complessità informativa dei teatri strategici che ci troveremo ad affrontare non potrà che crescere di conseguenza (tanto nel campo delle informazioni aperte quanto in quello delle informazioni riservate). Converrebbe affrontare il problema e discuterne fin d'ora. Prima di essere sorpresi dalla prossima revolution in intelligence affairs.

Note

1Per “macrosistema di sicurezza” intendiamo il network di tutte quelle entità che attraverso il complesso interagire delle loro azioni istituzionali con il tessuto culturale, sociale, economico, politico e istituzionale dello Stato, concorrono - più o meno direttamente e più o meno consapevolmente – al rafforzamento di tutte quelle azioni (istituzionali) che lo Stato stesso pone in essere ai fini della integrità della sua autonomia, dei suoi elementi costitutivi e delle sue funzioni originarie. Tale “macrosistema” comprende a grandi linee: a) i poteri effettivi dello Stato, b) le dipendenti strutture istituzionali, c) le cosiddette “infrastrutture critiche”, d) ogni organizzazione la cui attività si stima possa avere un riscontro significativo sul concetto di “sicurezza” ed e) l'insieme delle relazioni intercorrenti fra tutti questi soggetti. Tale definizione – dal carattere volutamente “universale” - comprende ovviamente gli Enti previsti dalla Legge n. 124 del 3 agosto 2008 costituenti il “Sistema di informazione per la sicurezza”.

2E pertanto “conveniente” - in termini di impegno di risorse umane, tecnologiche ed economiche - rispetto alla intelligence classificata.

3“Nuove architetture di intelligence alle porte” (Giovanni Nacci, su ANALISI DIFESA numero 36, Luglio/Agosto 2003 – Osservatorio Cesdis, pag. 7).

4Ed in realtà – per quel medesimo Ente – lo sono a tutti gli effetti.

5E non potrebbe essere diversamente, perché si finirebbe per comportarsi come quell'individuo che non sapendo dove custodire le chiavi della cassaforte che conteneva tutto il suo patrimonio... le ha chiuse dentro la cassaforte stessa.

6“So di non sapere”;, Socrate (Platone, Apologia)

7In altre parole, data una informazione da acquisire, non è possibile a priori né accertare, né escludere che essa esista o meno (o che sia disponibile o meno) nell'insieme “universale” delle fonti aperte. Mentre è possibile accertare o escludere con ragionevole certezza, se essa esista o meno nell'ambito di un determinato insieme di fonti/informazioni interne. A tal proposito giova ricordare che il fatto di poter accertare che una informazione esista o meno all'interno di un determinato insieme, è già di per se una informazione rilevante.

8Che è solo uno dei molti elementi qualificanti di una fonte/informazione.

9D'ora in poi per “Agenzia” si intenderà qualsiasi organizzazione, reparto o struttura governativa e/o istituzionale operante con funzioni di intelligence, anche non espressamente nominata dalla ultima riforma dei Servizi.

10E non è un caso che – nella realtà come nei film di spionaggio – si usa far riferimento ai Servizi anche con i termini “ditta” o “compagnia”.

11“Nuove architetture di intelligence alle porte” (Giovanni Nacci, su ANALISI DIFESA numero 36, Luglio/Agosto 2003 – Osservatorio Cesdis, pag. 7).

12Per chi volesse invece approfondire – in modo accessibile e spassoso - il fenomeno dell' overconfidence, consigliamo il libro “L'illusione di sapere: cosa si nasconde dietro i nostri errori” di Massimo Piattelli Palmarini, Mondadori, 1993.

13Sulla possibilità di riconfigurare la conoscenza, ossia di organizzarla in una pluralità di modi e punti di vista diversi, al fine di portare in superficie collegamenti e relazioni latenti, si basa ogni attività di intelligence.

14I vari segni e le relative grammatiche che normalmente usiamo per esprimerci nei vari idiomi.

15In particolare il text mining di ultima generazione.

16Nel senso mutato dal significato psicologico del termine che identifica un “...metodo di analisi [omissis] consistente nell’osservazione e nell’analisi dei propri contenuti [omissis] compiuta dal soggetto stesso e assunta come metodo di conoscenza” Dizionario On line della lingua italiana - De Mauro-Paravia

17Che, ci teniamo a dirlo, è cosa abbastanza diversa dal concetto di “total information awareness”.

18E quindi analisi, valutazione, categorizzazione, incrocio, confronto e impiego strategico delle informazioni disponibili.