

www.cesdis.it

OSSERVATORIO CeSDis

ANALISI DIFESA

Numero 36 anno 4 Luglio/Agosto 2003



www.analisdifesa.it

Nuove architetture di intelligence alle porte

di Giovanni Nacci

Nuove architetture di intelligence alle porte

nuovi modelli di intelligence e loro implicazioni tecnologiche

La pubblicazione dell'edizione italiana di un interessante volume sull'intelligence di Robert D. Steele¹ ha ridato vigore al dibattito sul riassetto dei servizi di informazione nel nostro paese. Vediamo in che modo la tecnologia è chiamata a coadiuvare le attività e le funzioni previste dai nuovi modelli organizzativi e strategici.

L'edizione italiana del volume di Steele "Intelligence " (prefazione del Senatore Francesco Cossiga) reca un'autorevole introduzione del Prof. Mario Caligiuri² il quale, nell'offerirci una sua interpretazione chiarificatrice circa i temi che saranno poi affrontati da Steele nel testo, dà particolare rilievo alla problematica della cosiddetta "intelligence delle fonti aperte" (OSINT³) quale strumento di accrescimento e completamento delle convenzionali attività di intelligence cosiddette "classificate".

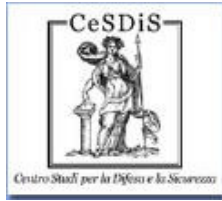
Nella sua introduzione, Caligiuri (che è anche curatore dell'edizione italiana) evidenzia giustamente la necessità di addivenire ad un serio dibattito sulle potenzialità dell'intelligence delle fonti aperte, anche e soprattutto sulla base di una attesa azione riformatrice dei "servizi" da inquadrarsi nel contesto più generale della trasformazione in senso federalista dello Stato. Egli propone inoltre (in linea con il processo di devolution avviato dal Governo, che prevede nuove e maggiori autonomie per le Regioni) l'ipotesi della costituzione di "...piccoli nuclei di intelligence regionali..."⁴ operanti al livello territoriale, sotto il coordinamento delle strutture di vertice (SISDe).

In altri e differenti contesti, il dibattito sull'intelligence si allarga anche verso orizzonti più lontani, con la proposta di realizzazione dell'E-CIA un organismo di intelligence centralizzato al livello europeo⁵. Da questi temi prendiamo lo spunto per fare alcune considerazioni legate alle implicazioni tecnologico-informative derivanti dalla applicazione di tali nuovi paradigmi organizzativi e strategici.

OSINT - Open Source Intelligence

Prima affrontare il tema specifico, è forse utile definire cosa si intende per "fonte aperta" e "intelligence delle fonti aperte". Molti autorevoli esperti hanno già definito con competenza e rigore scientifico il significato dei due termini e a questi facciamo riferimento per ogni esigenza che vada oltre gli scopi di questo lavoro. Noi però - per semplicità - utilizzeremo una definizione *non rigorosa*, semplificata, forse limitata, ma funzionale ai nostri scopi e che non contraddice le definizioni "accademiche".

Prioritariamente, l'intelligence da fonte aperta è "tutto ciò (attività, organizzazioni, sistemi, risorse, ecc.) che *non* prevede l'utilizzo e la trattazione di materiale classificato". Semplice no? Certamente, ma è ovvio che la definizione così com'è non semplifica più di tanto. Forse però, piuttosto che sul termine "intelligence", occorre soffermare di più l'attenzione sulla locuzione "fonte aperta"⁶.



www.cesdis.it

OSSERVATORIO CeSDis

ANALISI DIFESA

Numero 36 anno 4 Luglio/Agosto 2003



www.analisdifesa.it

Nuove architetture di intelligence alle porte

di Giovanni Nacci

L'errore più frequente è quello di confondere la fonte "aperta" con una fonte "gratuita". Non è automatico infatti che una fonte a pagamento non possa essere considerata *open*, o che si possa considerare tale solo quell'informazione che venga acquisita senza che sia resa necessaria una attività *volontaria, consapevole e mirata* di acquisizione: anche in questo caso è sbagliato considerare l'aggettivo "aperta" come sinonimo di "occasionale", "accidentale", "involontaria".

In linea di principio possiamo senz'altro dire che una fonte aperta può essere considerata tale quando 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. D'altro canto è importante evidenziare come non tutte le "fonti aperte" siano, per il semplice fatto di godere di questa peculiare caratteristica, automaticamente *utili, veritiere o affidabili* (aperto, gratuito, libero non sempre sono sinonimi di "vantaggioso").

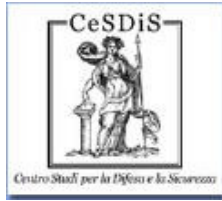
Un esempio che può contribuire a chiarificare il concetto è quello "del frutteto". In un frutteto solitamente i frutti crescono indisturbati sui loro alberi, i quali a loro volta affondano le proprie radici in un terreno di solito non recintato (magari confinante con una grande strada) comunque ben visibili e raggiungibile da chiunque. Con ogni probabilità quegli alberi e quei frutti saranno *formalmente* di proprietà di qualcuno. Qualcuno che li avrà coltivati, curati e che avrà speso risorse in termini di lavoro e denaro per farlo.

Ora, se rapportiamo il concetto di "informazione" ad un cesto di mele, ci troviamo di fronte ad una scelta con due sole possibilità:

- 1) entrare nel frutteto e raccogliere tranquillamente un cesto frutta da quegli alberi che consideriamo "fonte aperta" sulla base del fatto che sono lì, apparentemente incustoditi e disponibili per chiunque.
- 2) cercare il proprietario del frutteto, chiedergli di farci una buona offerta "un tanto al chilo" e comprare un bel cesto di mele.

Sia nel primo caso, in cui la *fruizione* del bene è stata assolutamente libera ed immediata (ammesso che riusciamo a farla franca dal pastore tedesco dell'agricoltore...) che nel secondo caso (dove si è resa invece necessaria una "*procedura*" e un "*corrispettivo*" per poter ottenere la merce) il fatto che quel frutteto sia sempre e comunque rimasto "open source" non cambia. Non cambia semplicemente perché quel frutteto erano *dall'inizio* predestinato a produrre beni che poi sarebbero stati venduti e/o distribuiti. La loro *destinazione originaria* era cioè proprio quella di essere scambiati senza ulteriori formalità, se non quella del pagamento di una giusta somma che ricambiassero il lavoro svolto dall'agricoltore.

La "prova del nove" l'abbiamo proseguendo con questo esempio naturalistico. Se al posto delle mele, all'agricoltore avete chiesto un mazzetto di quella graziosa piantina (vagamente assomigliante ad una della famiglia delle *cannabinacee*) che gli avete visto coltivare di nascosto nel giardino sul retro di casa sua... beh, quella piantina (quella... *fonte*) dovete per forza considerarla **non open source** e dovete parimenti accettare il fatto che quasi certamente non vi sarà mai veduta. Semplicemente perché *riservata* a scopi "particolari" e destinata ad essere smerciata e distribuita



www.cesdis.it

OSSERVATORIO CeSDis

ANALISI DIFESA

Numero 36 anno 4 Luglio/Agosto 2003



www.analisdifesa.it

Nuove architetture di intelligence alle porte

di Giovanni Nacci

attraverso canali altrettanto particolari, *riservati* - con tutta probabilità illegali - ma sicuramente "*chiusi*".⁷

Possiamo pertanto definire l'"intelligence delle fonti aperte" come quell'insieme di attività di intelligence aventi come materia prima fonti legalmente ottenibili e liberamente utilizzabili, immediatamente disponibili e acquisibili, o comunque ottenibili (anche dietro pagamento di un corrispettivo) da parte di una pluralità di soggetti che le detengono e che hanno interesse al libero scambio.

Come abbiamo visto, nella definizione di "intelligence delle fonti aperte" c'entra in qualche modo anche la tipologia del "canale" attraverso il quale queste informazioni vengono veicolate, canale che deve rispondere anch'esso ai requisiti del modello "open". La dottrina dell'OSINT è infatti caratterizzata da una sua "etica" incentrata sulla liceità della fonte dell'informazione, sulla legittimità della acquisizione e sulla legalità del canale attraverso la quale l'informazione è stata acquisita.

Ma vediamo ora quali implicazioni, trasformazioni organizzative, architetture e procedurali implicano i nuovi modelli di intelligence, sotto il punto di vista dell'infrastruttura tecnologica e informativa di supporto.

Intelligence regionale - citizen intelligence

Le peculiari caratteristiche dell'architettura ad *agenzie territoriali* prospettata dal Prof. Caligiuri, ci porta a considerare alcune tematiche di carattere immediato:

- 1) l'individuazione di una entità istituzionale cui l'agenzia locale per l'intelligence dovrà far capo (operativamente parlando);
- 2) l'identificazione dell'estensione dell'ambito informativo all'interno del quale l'agenzia dovrà porre in essere la propria attività;
- 3) l'identificazione di quei soggetti (istituzionali o meno) i quali dovranno essere accreditati quali "fornitori" di informazioni open source⁸.

Per quanto concerne il primo quesito (entità istituzionale responsabile dell'attività operativa) è attivo un esteso dibattito che non tarderà a dare i suoi frutti. Dal punto di vista prettamente "tecnico-informativo" sarà preferibile designare un'Autorità che possa vantare una consolidata esperienza nell'ambito del trattamento dell'informazione, soprattutto per quanto riguarda i modelli organizzativi ed i metodi operativi, con relativa disponibilità di infrastrutture tecnologiche e profili professionali adeguati.

Più difficile risulta delineare l'ambito informativo di competenza, ossia "quali e quante" tipologie di informazioni debbano essere trattate e con riferimento a quali temi. Nella rispettiva competenza territoriale, le agenzie regionali per l'intelligence dovrebbero poter effettuare (o concorrere ad effettuare) qualsiasi tipologia di intelligence, da quella economica a quella per la sicurezza, fermo restando il vincolo del trattamento delle sole fonti aperte. Una delle principali funzioni operative che queste strutture dovranno essere in grado di attivare è quella relativa alla *identificazione* dei



www.cesdis.it

OSSERVATORIO CeSDis

ANALISI DIFESA

Numero 36 anno 4 Luglio/Agosto 2003



www.analisdifesa.it

Nuove architetture di intelligence alle porte

di Giovanni Nacci

fornitori di OSINT sul territorio, alla loro *valutazione* ed alla creazione (e mantenimento) di un database dei soggetti più idonei (più *utili*) alla fornitura di informazioni aperte (centri di ricerca e studio, Università, Enti e amministrazioni locali/territoriali, imprese, ecc.).

Successivamente ognuna delle fasi del processo OSINT (*scoperta, distinzione, distillazione, distribuzione*⁹) potrà agevolmente essere riportata ad un contesto territoriale solo sulla base della territorialità del fornitore da cui l'informazione stessa proviene. Particolare attenzione però è da prestare - nel contesto specifico - all'ultima fase del processo OSINT: la *distribuzione*. Questa è la fase più delicata e critica di tutto il processo OSINT in quanto veicola il risultato ultimo di tutta la funzione di intelligence, dal sistema di produzione/scoperta (ossia chi ha condotto l'OSINT) al sistema decisionario (ossia chi sulla base di quelle risultanze dovrà prendere decisioni nel miglior modo possibile). Tale fase deve assicurare affidabilità, tempestività e sicurezza.

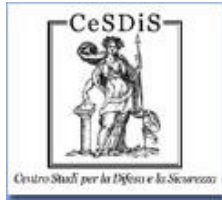
Nel caso di un network di agenzie regionali di intelligence, la fase di "distribuzione" effettuata dalle singole entità territoriali è da considerarsi in modo differente da come inteso convenzionalmente. Ciò perchè essa non fornisce immediatamente il risultato al "decisore", bensì ad un altro intermediario, ossia all'organismo di intelligence gerarchicamente superiore. Questo significa due cose:

- 1) la fase finale (*distribuzione*) dell'OSINT operata dall'agenzia regionale coincide - in una certa misura e per certi versi - con la fase OSINT iniziale (*scoperta*) operata dall'ente di intelligence centrale. Per quest'ultimo, l'agenzia regionale di intelligence, nei fatti non è altro che un "fornitore" OSINT privilegiato;
- 2) in questo passaggio è assai probabile che non possano essere del tutto verificate alcune delle garanzie prima citate necessarie per un OSINT funzionale e di qualità (affidabilità, velocità, tempestività).

Ed è proprio a questo punto che entra in gioco la progettazione dell'architettura delle infrastrutture tecnologiche ed organizzative che possiamo chiamare "*di trasporto*" (della conoscenza). Esse dovranno infatti adempiere al gravoso compito di veicolare la conoscenza così com'è, scongiurando ogni contaminazione, rispettando strettamente i requisiti richiesti. Il modello necessita della creazione di un network (tecnologico sì, ma soprattutto organizzativo) così avanzato da far apparire le varie basi di dati come fossero un'*unica conoscenza centralizzata*. I principali (irrinunciabili) requisiti richiesti al progetto dovranno pertanto essere:

- a) immediata disponibilità delle informazioni dalle/alle singole unità territoriali di OSINT;
- b) strettissimo controllo del livello di ridondanza di dati e informazioni;
- c) nessuna ambiguità semantica o sintattica all'interno della "conoscenza";
- d) nessuna autoreferenzialità delle singole agenzie territoriali.

Per far sì che questi requisiti vengano tutti verificati, il network deve avere unità di metodi, modelli e procedure: *metodi* per l'accesso condiviso alla conoscenza preservandone l'originalità, l'autenticità e la riservatezza; *modelli* per la pianificazione strategica delle relazioni semantiche fra entità informative multimediali; *procedure* comuni rigidamente formalizzate ai fini di ogni operazione di



www.cesdis.it

OSSERVATORIO CeSDis

ANALISI DIFESA

Numero 36 anno 4 Luglio/Agosto 2003



www.analisdifesa.it

Nuove architetture di intelligence alle porte

di Giovanni Nacci

"trattamento" delle informazioni (aggiornamento, cancellazione, integrazione, correzione, correlazione, ecc.).

L'informazione dovrà inoltre essere accuratamente categorizzata e dovrà essere attentamente (e *continuamente*) monitorato il tasso di *ridondanza* dei dati, affinché sia sufficiente a:

- 1) assicurare l'integrità sintattica dei dati e delle informazioni;
- 2) assicurare un elevato tasso di disponibilità delle informazioni anche in presenza di un alto numero di istanze di accesso concorrenti;
- 3) permettere l'accesso alla conoscenza mediante un approccio di tipo tematico e non solo mediante "keyword" (parole chiave);

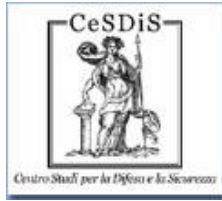
Tutto ciò, cercando accuratamente di evitare qualsiasi tipo di ambiguità semantica e autoreferenzialità dell'informazione

Ovvio che un database relazionale multidimensionale distribuito come quello di cui trattasi, dovrà essere dotato di strumenti di *estrazione* della conoscenza allo *stato dell'arte* (data mining), così come allo stato dell'arte dovranno essere le caratteristiche operative di sicurezza di tale network di conoscenze, parametro quest'ultimo tutt'altro che facilmente implementabile.

E' infatti importante sottolineare che pur prevedendo l'OSINT l'analisi di fonti aperte *non classificate*, è del tutto probabile che i risultati di quelle analisi debbano invece giovare di una classificazione di riservatezza. Ciò genera un notevole problema tecnologico di sicurezza, sia all'interno delle singole organizzazioni periferiche, sia nei suoi rapporti istituzionali di interscambio di informazioni con gli enti centrali di sicurezza (si è detto il SISDe) ma anche i reparti di intelligence degli altri ministeri e/o Forze Armate.

Mai quanto in questo caso, vale il vecchio adagio della sicurezza informatica secondo il quale il livello di sicurezza di un sistema di informazioni è inversamente proporzionale al grado di *disponibilità* di accesso alle risorse che si concede agli utenti. Ovvio infatti che più un sistema è concesso in uso ad un numero elevato di utenti, tanto più difficile è soddisfare i requisiti di sicurezza.

Appare chiaro infine come un modello tanto articolato e complesso, non possa prescindere da una diffusa e attenta opera di *training* di tutti i soggetti che vi interagiranno. Ciò significa selezione, formazione, educazione, indottrinamento, sensibilizzazione, comunicazione. "*Selezione e formazione*" di coloro che saranno gli "addetti ai lavori", provenienti da enti civili e militari (forze armate, forze di polizia, ecc.) ma anche reclutati nelle università e nei centri di ricerca; "*educazione e indottrinamento*" per quelle realtà che saranno identificate come fonti dell'OSINT (imprese, aziende, professionisti, centri di ricerca, media, ecc.), quindi "*sensibilizzazione e comunicazione*" all'opinione pubblica, per lo sviluppo di una cultura dell'intelligence delle fonti aperte che ne evidenzii opportunità, finalità, moralità, trasparenza e che sottolinei al contempo l'importanza e la necessità dell'intelligence "classificata".



www.cesdis.it

OSSERVATORIO CeSDis

ANALISI DIFESA

Numero 36 anno 4 Luglio/Agosto 2003



www.analisdifesa.it

Nuove architetture di intelligence alle porte

di Giovanni Nacci

Questa complessa e fondamentale fase di preparazione è essa stessa un network; un network di attività, conoscenze, idee, eventi, progetti. Su di essa è già possibile ipotizzare un'infrastruttura tecnologica di supporto alla conoscenza, ma è certamente solo dopo che sarà possibile pensare con efficacia a quelli che potremmo chiamare "modelli comuni per la rappresentazione della conoscenza condivisa".

L'altra faccia della medaglia: il progetto E-CIA

L'E-CIA "European Central Intelligence Agency", è un programma di ricerca capitanato dal *team* dell'E-CIA Project (www.departamentofintelligence.com/e-cia) volto allo sviluppo di un progetto preliminare per la realizzazione – al livello europeo - di una struttura di coordinamento delle attività d'intelligence poste in essere dai singoli paesi partner. All'E-CIA Project partecipano con il loro contributo alcuni tra i più autorevoli esperti del settore, tra i quali lo stesso Steele.

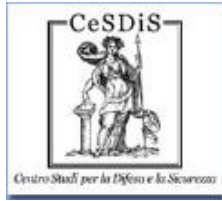
L'obiettivo è la creazione di un'autorità europea per l'*alto coordinamento* delle attività di intelligence dei singoli paesi partner, che costituisca una risposta ai cambiamenti (passati, presenti e futuri) del teatro strategico europeo anche – e soprattutto - in relazione alla primaria esigenza di fronteggiare con efficacia il terrorismo internazionale e le criminalità organizzate transnazionali.

Sotto l'aspetto *informativo*, tale processo paradossalmente comporta - su scala internazionale - problematiche del tutto assimilabili a quelle evidenziate dal modello dell'intelligence territoriale del Prof. Caligiuri.

Infatti, se la principale funzione dell'E-CIA dovrà essere (come sarà) quella di *alto coordinamento strategico*, essa dovrà di fatto operare una sorta di "*intelligence sull'intelligence*" nei confronti della singole agenzie dei paesi partner. Affinché l'E-CIA possa esprimere concretamente una reale politica di *intelligence comunitaria* (con l'obiettivo tra l'altro di scongiurare ulteriori *fallimenti dell'intelligence*, come si è detto dell'11 settembre) occorre che le singole nazioni accettino e riconoscano come indispensabile - in un contesto di volontaria e consapevole adesione ad un nuovo assetto strategico dell'Europa - la *partecipazione* nelle loro attività di intelligence di un ente superiore.

Il che significherà, per forza di cose, entrare nel merito di valutazioni, scelte, decisioni e indirizzi strategici dell'attività delle singole agenzie nazionali. Tale compartecipazione, dovrà concretizzarsi in un "sistema di relazioni di fiducia¹⁰" tale che chi avrà l'onere dell'alto coordinamento (l'E-DCI¹¹), possa disporre in tempo reale della *cognizione* di tutta la conoscenza utile disponibile in quell'istante, riguardo una specifica esigenza.

Ciò significa che sarà necessario conoscere - *tempestivamente e on demand* - "dove" risiedono le informazioni di cui si ha bisogno, "chi" ne è il legittimo proprietario (o fornitore) e "da chi" ottenere invece quelle informazioni che non è stato possibile reperire all'interno del sistema. In altre parole un management talmente avanzato da costituire un sistema di *percezione, osservazione, analisi e generazione di conoscenza*.



www.cesdis.it

OSSERVATORIO CeSDis

ANALISI DIFESA

Numero 36 anno 4 Luglio/Agosto 2003



www.analisdifesa.it

Nuove architetture di intelligence alle porte

di Giovanni Nacci

Conclusioni

Qualcuno avrà forse notato come questo lavoro costituisca, per certi versi, l'ideale prosecuzione (e conclusione) del discorso iniziato con i precedenti articoli “*Database, Sicurezza e Sovranità*” e “*Text Mining nelle applicazioni per la sicurezza*”.

In realtà la trilogia si è delineata in modo del tutto spontaneo, tant'è che ogni singolo articolo può essere autonomamente valutato anche fuori dal contesto degli altri. Tuttavia, è innegabile il fatto che i tre lavori facciano parte di uno stesso "cammino" che ho avuto l'opportunità di percorrere in prima persona, grazie soprattutto agli autorevoli esperti che hanno accettato di contribuire alla mia modesta opera di ricerca ed ai quali va il mio più profondo riconoscimento.

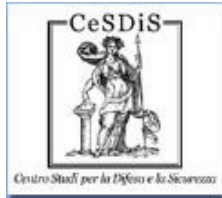
Volendo in ogni caso tentare un'interpretazione omnicomprensiva, posso forse dire che i tre lavori affrontano quelle che in futuro saranno probabilmente le tematiche sulle quali si svilupperà il nuovo modello dello *strumento di intelligence* e più in particolare in relazione:

- 1) alla tutela della conoscenza *utile* rappresentata da tutte le componenti (istituzionali e non) di una organizzazione (Stato, Unione, o impresa che sia) e all'esercizio della *legittima sovranità* su di essa;
- 2) alla ricerca dell'*eccellenza* nelle attività tecnico-informative di captazione, analisi e valutazione dell'informazione (data mining, text mining);
- 3) alla realizzazione dell'*alto indirizzamento e coordinamento strategico* comune di ogni risorsa informativa (istituzionale o meno) utile alla tutela della sicurezza e della democrazia.

Sempre più spesso quando si affrontano questi temi si conclude facendo riferimento alla cosiddetta *overdose di informazioni*, che starebbe per saturare le attuali capacità tecnologiche di analisi. A mio parere database, reti, sistemi e infrastrutture tecnologico-informative hanno ben poca utilità se non riusciamo a percepire il significato *utile* di tutta la conoscenza che in esse riversiamo. Infatti, il confine tra “conoscenza” e “*illusione della conoscenza*” è sempre molto labile e si rischia di credere di essere nell'una, quando in realtà si è nell'altra.

Ringraziamenti

Desidero ringraziare il Prof. Mario Caligiuri e il Prof. Francesco Sidoti per la squisita disponibilità nel “condividere” la loro autorevole conoscenza e per l'appassionata opera di formazione e sensibilizzazione sulle tematiche dell'intelligence. Ringrazio inoltre Charles P. Rault e il Dott. Marco Giaconi del CeMiSS per la sua attività di studio e ricerca sull'European Central Intelligence Agency, oltre che per avermi voluto coinvolgere in prima persona nel progetto E-CIA. Ringrazio tutti coloro che – professionisti o “dilettanti”¹² - si occupano delle tematiche relative all'intelligence ed alla sicurezza, nella speranza che la “condivisione” di questo mio personale contributo, gli possa essere in qualche modo utile e proficua. Un grazie particolare va alla Dott.ssa Antonella Lupo per il suo insostituibile supporto e la collaborazione nella interpretazione dei testi in lingua inglese.



www.cesdis.it

OSSERVATORIO CeSDis

ANALISI DIFESA

Numero 36 anno 4 Luglio/Agosto 2003



www.analisdifesa.it

Nuove architetture di intelligence alle porte

di Giovanni Nacci

Note:

¹ Robert David Steele "Intelligence, Spie e segreti in un mondo aperto" - Rubbettino 2002

² Autorevole esperto di tematiche di intelligence, docente di comunicazione pubblica all'Università della Calabria.

³ OSINT: Open Source Intelligence, intelligence delle fonti aperte

⁴ ADNKRONOS (Cosenza-19.12.2001) "Servizi: Caligiuri, intelligence anche a livello regionale".

⁵ "ECIA" (*European Central Intelligence Agency*). A tal proposito si veda anche "European Director of Central Intelligence: a proposal" di Marco Giaconi (CeMiSS) in www.departmentofintelligence.com/e-cia.

⁶ anche "open source"

⁷ non ce ne vogliono gli agricoltori, è solo un esempio.

⁸ si segue a tal proposito la dottrina indicata da Steele, secondo la quale l'OSINT deve procurare informazioni "appena sufficienti, appena in tempo" operazione in cui il valore aggiunto dell'OSINT sta proprio nel saper "dove cercare" le informazioni di cui si ha necessità (fase di selezione della fonte). In tale contesto Steele dà particolare importanza alle risorse di strutture private già presenti e operanti nei vari campi specifici.

⁹ R.D. Steele, opera citata pag. 193.

¹⁰ TRN- Trust Relationship Network

¹¹ E-DCI – European Director of Central Intelligence

¹² Francesco Cossiga "Abecedario, per principianti, politici e militari, civili e gente comune" – Rubbettino 2002