DE GRUYTER
OPEN

Research Article

The Intelligence Process and the Information Management

Antonella Colonna Vilasi[1]

Centro Studi Uni, Italy

Doi: 10.2478/ajis-2018-0001

Abstract

The Intelligence cycle is a procedure framework for the development of mission-focused Intelligence support. It is not an end in itself, nor should it be viewed as a rigid set of procedures that must be carried out in an identical manner on all occasions. The commander and the Intelligence officer must consider each IR (Intelligence requirement) individually and apply the Intelligence cycle in a manner that develops the required Intelligence in the most effective way (U.S. MARINE CORPS, 2007).

Keywords: *Intelligence; Security; Intelligence Cycle; Politics; Society*

1. Introduzione

Quando si parla di ciclo informativo si fa riferimento «alle architetture distributive e ai percorsi che i vari prodotti dell'Intelligence (riviste, rapporti, avvisi, previsioni) prendono all'interno dell'amministrazione (*Intelligence Cycle*)» (Castelvecchi, Lo Re, Zardo, 2002).

Si legge: "The Intelligence cycle is a procedure framework for the development of mission-focused Intelligence support. It is not an end in itself, nor should it be viewed as a rigid set of procedures that must be carried out in an identical manner on all occasions. The commander and the Intelligence officer must consider each IR (Intelligence requirement) individually and apply the Intelligence cycle in a manner that develops the required Intelligence in the most effective way" (U.S. MARINE CORPS, 2007).

A parte le varie considerazioni, propedeutiche a qualsiasi discorso sul ciclo informativo bisogna fare una seppur breve digressione volta a chiarire concetti come dati, notizie, informazioni.

Per fatto o avvenimento s'intende qualsiasi evento o azione che si è potuto appurare che esiste e/o che si è verificato ed alla cui conoscenza si attribuisce un valore informativo.

La notizia è la cognizione non elaborata di un fatto e/o di un avvenimento significativo relativo ad argomenti d'interesse; l'informazione, a sua volta, è il prodotto scaturito da una notizia a seguito di un processo di elaborazione, analisi, interpretazione, comparazione, integrazione ragionata e valutazione.

[1] *Pioniera degli studi di Intelligence in Italia e studiosa di Intelligence, ha pubblicato più di 70 libri sulla materia. Tra cui: The Intelligence cycle, The History of M16, The History of the CIA, The History of the Italian Secret Services, The History of the Entity, The History of Mossad, and the History of the STASI. - Pioneer in Intelligence Studies in Italy, the author's research interests focused on Intelligence, the relation with the Political Science and the Intelligence cycle. With more than 70 books published on the topics; among them: The Intelligence cycle, The History of M16, The History of the CIA, The History of the Italian Secret Services, The History of the Entity, The History of Mossad, and the History of the STASI.*

2. Metodi di Ricerca

Questo studio utilizza un approccio metodologico in tre fasi: raccolta, codifica e analisi dei dati, utilizzando tecniche qualitative.

L'articolo offre numerosi contributi originali alla letteratura scientifica di settore.

In primo luogo, riesamina le fonti e la costruzione teorica e propone alternative alla letteratura scientifica di riferimento.

Rafforza le interrelazioni olistiche in termini di coerenza tra discipline quali Intelligence studies, sociologia, geografia politica e scienze politiche.

In terzo luogo, i metodi misti proposti generano un'agenda per possibili studi e ricerche future.

I documenti utilizzati si riferiscono a Open Source, archivi, pubblicazioni e fonti secondarie affidabili.

Il limite di questa ricerca è dovuto al fatto che l'Intelligence Cycle dovrebbe essere trattato in un intero volume e non solo con un breve articolo.

3. Risultati Investigativi

Le informazioni, pertanto, devono essere caratterizzate da:

- certezza, devono, cioè, essere oggettive e, qualora non siano tali, questo deve essere segnalato;
- completezza, per quanto possibile nessun elemento utile deve essere trascurato;
- organicità, i singoli elementi vanno ricondotti fino alla struttura generale, con riferimento ad elementi di collegamento concreti e provati;
- compatibilità, nel quadro informativo completo, su una data situazione, non vi devono essere questioni discordanti e qualora alcune di esse possano far emergere una divergenza, vanno rivalutate;
- interpretazione, ogni notizia va analizzata nella sua completezza e, qualora si presti a più valutazioni, queste vanno differenziate;
- attribuibilità, le notizie, ove possibile, devono essere collegate ad una fonte individuata o certamente individuabile;
- temporizzazione, gli elementi informativi devono essere datati e, qualora la loro valenza si protragga nel tempo, essa va delimitata;
- localizzazione, i dati acquisiti devono essere collocati con precisione nello spazio geografico cui si riferiscono;
- novità, i dati finali prodotti dal processo informativo non devono riferirsi a cose ovvie o già acquisite precedentemente (SCUOLA DI GUERRA-COMANDO C4IEW, 1999).

Chiariti questi punti possiamo tentare di capire come queste diverse modalità di “informazioni” entrano di diritto nel ciclo informativo.

Iniziamo col dire che l’*Intelligence* può essere paragonata a una società di servizi che riceve un input in seguito a una richiesta dal decisore; al termine di un lungo processo, detto appunto informativo, le notizie raccolte, sotto forma di output, si trasformano in un’informazione che viene poi vagliata, elaborata, analizzata ed inserita in un contesto di scenario.

Il termine “processo” o “ciclo informativo” può essere usato indistintamente visto che la natura dell’attività informativa è quella di un procedimento ciclico, senza soluzione di continuità; dal che ne deriva che la gestione dell’attività d’Intelligence deve essere intesa come un procedimento permanente e sistematico che non ha un termine definito e questo in virtù del fatto che le conclusioni e le informazioni prodotte diventano, a loro volta, le basi per ulteriori attività di ricerca.

3.1 Il ciclo Intelligence

Il ciclo è predisposto per la gestione in tempo reale di qualsiasi dato e notizia sull’avversario, dato che le attività condotte sono interconnesse e finalizzate ad acquisire, collazionare, elaborare, valutare e diffondere informazioni, utili al perseguimento dello scopo del richiedente il servizio, lo Stato.

Ai fini operativi è irrilevante se le finalità sono preventive, quale mera espressione del *need to know*, o repressive, con la panoplia di misure di controintelligence.

Nel suo evolversi il processo si ripresenta, quindi, sistematicamente poiché gli elementi non approfonditi o eseguiti nelle attività precedenti possono costituire, a ragion veduta, il presupposto per la prosecuzione in profondità di altre successive indagini (Eftimiades, 1994).

Il ciclo informativo può essere suddiviso in una serie di fasi: la fase concettuale o "direttiva", la fase di pianificazione, l'acquisizione dei dati, la raccolta dei dati e la loro analisi, ed infine la loro valutazione.

La prima fase rappresenta un momento di particolare importanza, visto che è lo step in cui si inizia l'analisi della situazione per giungere all'individuazione dei dati utili alla definizione degli "obiettivi informativi" da conseguire.

Nel caso in cui i dati raccolti si dimostrino insufficienti si procede all'individuazione degli "indizi", ovvero di elementi provvisori che, posti come ipotesi di lavoro, si possono successivamente trasformare in "obiettivi" oggetto dell'attività di ricerca.

Il successivo momento della "pianificazione" ha lo scopo di assegnare "obiettivi" d'informazione, con particolare riguardo alle capacità ed all'efficienza.

Nell'ambito della pianificazione andranno indicate le fonti più idonee da attivare e utilizzare, poiché, presumibilmente, in grado di fornire dati pertinenti.

Nella distribuzione degli obiettivi si dovrà considerare opportuna l'assegnazione, per quanto possibile, dello stesso obiettivo a più organi e fonti, in modo da avere notizie di differente provenienza, da confrontare e verificare con riscontri incrociati.

Conclusa la pianificazione della raccolta si giunge al vero e proprio invio degli ordini e delle richieste alle fonti ed agli organi di ricerca.

L'organizzazione della ricerca consiste nell'individuare gli elementi essenziali d'informazione, come gli aspetti riguardanti l'ambiente dell'avversario, le eventuali incognite che possono condizionare la scelta della linea di azione (competenze fondamentali dell'unità di ricerca) e i fattori esterni all'indagine che possono compromettere la riuscita dell'operazione.

In questa fase si rivela fondamentale la figura dell'analista.

Una volta esaurita la fase di ricerca si passa alla "raccolta dei dati", che consiste nelle operazioni di "trasmissione" delle notizie da parte degli organi di ricerca all'organo informativo deputato alla relativa "registrazione".

Perfezionata la fase organizzativa e di ricerca del processo informativo, inizia la fase dell'analisi propriamente detta, il momento valutativo vero e proprio della produzione.

Se la raccolta e la ricerca delle informazioni è stata fatta in modo preciso ed esaustivo è possibile sviluppare un'analisi efficace e completa.

Sotto l'aspetto concettuale l'analisi si compone delle seguenti fasi:

- esame preliminare;
- valutazione del dato informativo;
- integrazione-interpretazione;
- trascrizione ed archiviazione.

L'"esame preliminare" consiste in un primo vaglio della comunicazione volto a rilevare se la stessa sia completa in ogni sua parte, se i dati contenuti siano di urgente diramazione tali da consigliarne l'immediata diffusione, senza valutazione e interpretazione, se debbano essere elaborati prioritariamente per la distribuzione, se rivestano un interesse informativo e, infine, se non siano di alcun interesse.

Questa fase, pertanto, permette d'individuare le potenzialità della notizia e sviluppare una sommaria ricognizione delle ipotesi di approfondimento praticabili.

Nella valutazione dei dati informativi, sia in ambito civile sia militare, viene utilizzato un sistema di catalogazione alfa-numerico che tiene conto sia dell'"attendibilità" della "fonte" o dell'organo di ricerca, sia della "veridicità" della notizia. La verifica delle fonti, infatti, è una delle fasi più delicate (Gagliano, 2011).

3.2 Fonti e Sistemi informativi

Parlare di fonti e di Sistemi informativi significa fare riferimento a diversi tipi di informazioni: tradizionali, aperte, riservate, libere, interne ed esterne.

Si deve aggiungere un ulteriore livello di classificazione, visto che le fonti possono essere rilevanti e irrilevanti, e avere un buon rapporto tra costi e benefici.

Insomma, come per tutto ciò che riguarda i sistemi informativi, anche la questione delle fonti si risolve in un ginepraio di informazioni, possibilità e alternative.

Come avremo modo di evidenziare, la questione delle fonti e le loro modalità di reperimento è talmente complessa che si è reso necessario identificare per ogni momento della "raccolta" delle fasi precise.

Parleremo, infatti, di "scoperta", "distinzione", "distillazione" e "distribuzione" di fonti (Steele, 2002).

Nell'ambito dell'Intelligence il termine "fonti d'informazioni" definisce "una persona o una cosa (documenti e/o materiali) da cui si ottiene l'informazione".

Una fonte può essere a sua volta:

- controllata, quando viene attivata per fornire risposte a specifiche domande;
- non controllata, quando fornisce informazioni ma su di essa non può essere esercitato alcun controllo;
- aperta, in questo caso si tratta di un tipo di fonte non controllata che fornisce informazioni relative al background (*basic intelligence*) e informazioni sulla situazione in atto (*current intelligence*);
- casuale, quando un individuo fornisce spontaneamente un'informazione senza che la medesima sia stata richiesta (www.sicurezzanazionale.gov.it/web.nsf/pagine/glossario-intelligence, 2017).

Le fonti d'informazione, aperte o chiuse, sono importanti nel contesto della ricerca. Le prime, in particolare, possono essere costituite da archivi e schedari informatici; la fonte aperta può anche essere tratta da giornali, riviste, pubblicazioni scientifiche, relazioni ufficiali di dibattiti governativi di pubblico dominio.

Nei Paesi democratici, dove non vi sono limitazioni alla libertà di stampa e di pubblicazione di notizie politiche e scientifiche, la raccolta di informazioni aperte risulta molto utile perché consente di avere un quadro completo, aggiornato e abbastanza attendibile della situazione nei diversi settori.

Le fonti chiuse, invece, sono quelle la cui accessibilità è vietata, oggetto, quindi, di specifica attività di spionaggio o intercettazione, condotta sia da persone sia attraverso mezzi tecnici; in questo caso per entrare in possesso di queste fonti è necessario poter contare su una fitta ed efficace rete informativa fatta di specialisti e di apparecchiature sofisticate atte a rilevare gli eventi e trasformarli in segnali interpretabili (Izzi, 2011).

Gli studiosi del settore usano classificare le modalità per reperire informazioni in due grandi categorie: *Human Intelligence* (HUMINT), informazioni ottenute da fonti umane e la *Signals Intelligence* (SIGINT), che fa riferimento a quella parte dell'*Intelligence* riferibile ad aspetti e strumenti prettamente tecnologici.

Accanto alle sopra citate categorie si sta imponendo anche la cosiddetta *Open Source Intelligence* (OSINT) che non è riconducibile a nessuna delle due categorie precedenti, sebbene necessiti di entrambe:

> *"OSINT integrates world class human expertise with an integrated human-technical process to produce just enough, just in time Intelligence – information tailored to support a specific decision"(Quigging, 2007).*

La preferenza per l'uno o l'altro sistema dipende dalle priorità informative che ogni epoca storica manifesta.

La più prevedibile tra le minacce alla nostra sicurezza è costituita, a parere di molti esperti, dalla proliferazione delle armi di distruzione di massa, utilizzabili anche da piccoli gruppi terroristici.

Per questo tipo di minacce è necessario disporre maggiormente perlopiù di fonti HUMINT e OSINT.

La HUMINT rappresenta l'insieme di tutte le informazioni ottenute attraverso fonti umane, cioè attraverso informatori o interrogatori e monitoraggi di persone che per motivi istituzionali o professionali sono a conoscenza delle informazioni che si vogliono reperire.

Si tratta, senza dubbio, del sistema di raccolta informativa più antico e più rischioso, capace di assicurare una copertura anche in aree impenetrabili da altri sistemi.

Molto in voga nel periodo della Guerra fredda, questa tecnica è stata per un certo periodo messa in ombra dagli strumenti di raccolta tecnologica, ma, recentemente, proprio in un mondo multipolare, ha dimostrato di rivelarsi uno strumento estremamente efficace e versatile.

Come per ogni altra attività umana, tuttavia, anche questa modalità di acquisizione dati ha i suoi aspetti negativi.

L'intervallo di tempo fra la rilevazione, la verifica e il rapporto può essere talmente lungo da vanificare l'utilità dell'informativa d'Intelligence.

Altro grave difetto è rappresentato dall'influenzabilità sia dell'agente che dell'informatore, con evidenti ripercussioni sulla credibilità dell'informativa che, per altro, difficilmente può essere verificata (Izzi, 2011).

L'alternativa è rappresentata dalla *Signals Intelligence* che si presenta come uno strumento duttile con diverse modalità d'impiego dettate sia dalle specifiche esigenze d'Intelligence che dal tipo di rilevatori che si hanno a disposizione.

Si pensi al seguente esempio: in tempo di guerra le decisioni sul campo di battaglia subiscono condizionamenti significativi in ragione di rilevamenti satellitari, di rilievi fotografici su bande luminose differenti, ultravioletti o infrarossi, di segnali radar o sonar in ambiente marino, senza dimenticare l'utilità delle intercettazioni e decodifica delle comunicazioni del nemico, la *Communication Intelligence* (Comint).

"Lo scenario, come scrive Johnson, si modifica, il nemico del mio nemico non è più necessariamente mio amico. Specialmente nel settore economico tutti spiano, o tentano di spiare, tutti" (Johnson, 2000).

Gli esperti classificano la SIGINT secondo il tipo d'informazione che riesce a rilevare.

La *Measurement and Signature Intelligence* (MASINT) comprende le misurazioni che i sensori sono capaci di raccogliere, eccetto le comunicazioni e le rilevazioni fotografiche (rispettivamente COMINT e *Imagery)*.

L'*Imagery* è stata di primaria importanza durante la Guerra fredda per il controllo degli armamenti e la dislocazione degli arsenali atomici e convenzionali dell'avversario.

Sul piano tattico l'*Imagery* si è dimostrata uno strumento indispensabile per limitare le perdite sia fra i militari che fra i civili della parte avversa (Johnson, 2006).

Uno studio realizzato alla fine della Prima guerra del Golfo dal Congresso degli Stati Uniti ha segnalato l'importanza dell'utilizzazione dei sistemi JSTARS, l'ASARS e L'UAV.

Il primo è riuscito a fornire ai responsabili delle operazioni, indipendentemente dalle condizioni meteorologiche, informazioni sugli obiettivi da colpire; il secondo ha permesso di detectare target fissi, sia nelle ore notturne che diurne; mentre il terzo, utilizzato in quell'occasione per la prima volta, è riuscito a produrre preziosissime mappe del terreno per le unità della Marina, dell'Esercito e per quelle anfibie senza rischiare la perdita di un solo pilota.

La mappatura del terreno per finalità tattiche (1:50.000) richiede, infatti, immagini riprese a bassissima quota e le operazioni di volo in queste situazioni espongono il velivolo ed il suo pilota ad un alto rischio di abbattimento.

Tuttavia l'*Imagery* non è più monopolio esclusivo delle superpotenze; esistono, infatti, sul mercato aziende in grado di fornire a poco prezzo immagini con una risoluzione ad un metro (Asker, 1994).

I componenti principi della SIGINT sono i sensori deputati alla rilevazione e ne esistono di due tipi:

- presidiati, quelli che prevedono la presenza dell'uomo per l'utilizzazione dello strumento,
- e quelli non presidiati, che vengono abbandonati sul suolo o negli oceani e che comunicano con il centro di comando attraverso segnali radio.

Gli *Unattended Ground Sensors* (UGS) sono sicuramente i più diffusi.

Si distinguono in acustici, sismici, magnetici, radiologici ed elettro-ottici, ed hanno il pregio di avere capacità d'Intelligence istantanea, rilevare movimenti che non possono essere scoperti in altro modo e non mettere a rischio vite umane.

Di contro risentono dei disturbi provenienti da installazioni vicine, devono essere camuffati per evitarne l'individuazione, potrebbero mandare informazioni errate in caso di malfunzionamento, e richiedono un sistema sofisticato di analisi per l'interpretazione dei dati acquisiti (Carapezza, Law, Stalker, 1999).

Come spiega Izzi: "Il primo passo nell'attività di Intelligence viene fatto da tutti nel settore delle fonti aperte".

Le fonti aperte, come prosegue Izzi, non sono più un settore di esclusiva pertinenza dell'Intelligence essendo diventate uno strumento fondamentale anche per molti altri ambiti, tra cui quello privato e aziendale.

Gli studiosi d'Intelligence distinguono tre categorie concettuali di fonti aperte:

- l'*Open source data*, Osd, informazioni semplici ed immediate, come i dispacci di agenzie, fotografie, immagini satellitari commerciali, lettere personali, interrogatori;
- l'*Open source information*, Osif, dati assemblati generalmente da una selezione editoriale, che formano un corpo unitario di notizie, possibilmente verificate, come i giornali, i libri, le pubblicazioni scientifiche;
- l'*Open source intelligence*, Osint, notizie deliberatamente ricercate, discriminate fra le tante, analizzate e disseminate ad un pubblico selezionato (Kock, 2011).

La convinzione fin troppo diffusa che le fonti aperte non siano che una mera raccolta di ritagli di giornale o una navigazione più o meno attenta su Internet trae in inganno moltissime persone, specialmente gli addetti all'intelligence.

Il dottor Assen Marcevski, ufficialmente interprete presso l'ambasciata bulgara a Roma, ma in realtà spia del suo governo, nel suo libro tratto da memorie operative *Misteri italo-bulgari*, racconta di come moltissime informazioni provenissero dalla rassegna stampa di alcuni giornali minori e dei giornali di partito, specie di quelli appartenenti a gruppi extraparlamentari.

Marcevski riteneva quelle notizie «importantissime, sommariamente verificabili con interviste a persone "dell'ambiente"».

> *"Un'edizione provinciale specializzata pubblica delle previsioni politiche o critiche sulla strategia economica italiana nei confronti degli Usa o dell'Unione Sovietica; [...] se poi si vuole che il "riservato" sia fatto a dovere, si attacca discorso con un qualunque italiano che lavori in quel determinato settore. Non si deve tempestarlo di domande: gli italiani sono loquaci, quando si mettono a parlare non la smettono più" (Marcevski, 2002).*

È certamente un approccio ancora un po' troppo rozzo per poter parlare di Osint, ma l'idea di reperire informazioni utili dalla stampa è senz'altro valida.

Inoltre a livello etico nessuno potrà recriminare a un'agenzia di aver rubato notizie quando erano alla portata di tutti in un giornale, o aver utilizzato immagini satellitari fornite da ditte autorizzate, come potrebbe essere un banalissimo *Google Earth*.

Tra i vantaggi delle fonti aperte c'è di sicuro l'immediatezza della disponibilità informativa al verificarsi di una crisi.

La maggior parte delle situazioni di emergenza si verificano nei Paesi considerati di secondaria importanza, che non sono coperti da capacità di raccolta classificata.

Queste situazioni di emergenza comportano un'eccessiva fiducia nelle organizzazioni internazionali e, come conseguenza, dover condividere informazioni con alleati di dubbia affidabilità.

Tutto ciò, se non impossibile, è quanto meno molto difficile nel caso di fonti classificate.

Non va dimenticato, infatti, che con l'Osint si ottengono principalmente risultati che non necessariamente devono possedere classifiche di segretezza (Steele, 2002).

L'Osint può risultare fondamentale anche come strumento ai fini di operazioni militari.

Un ufficiale americano, comandante di stormo dell'Aviazione della Marina, alla guida del primo bombardamento di Bagdad durante la Prima guerra del Golfo, asserisce a riguardo delle fonti

aperte:

> *"Se esse sono accurate all'85%, se sono tempestive e posso condividerle, questo è per me molto più utile di quanto lo sia un manuale d'informazioni classificato Top Secret che è troppo voluminoso, intempestivo, e richiede una cassaforte e tre ufficiali della sicurezza per essere trasportato sul campo di battaglia" (Steele, 2002).*

Occuparsi di OSINT significa mantenere i contatti con gli esperti della materia o nel particolare settore d'interesse del momento, così da poterne avere vantaggio se necessario:

> *"Nel XXI secolo, l'apice dell'abilità per il migliore degli analisti consiste nell'essere in grado di mettere il politico che abbia una questione scottante rapidamente in contatto con un esperto a livello mondiale, generalmente del settore privato, che possa offrire le informazioni richieste subito e in pochi minuti" (Steele, 2002).*

Ulteriore vantaggio delle fonti esterne è che la formazione e la competenza di tali esperti sono un costo di competenza altrui, che non pesa sul budget se non nella misura della singola informazione.

Nessuna agenzia governativa dovrà mantenere del personale da aggiornare continuamente e, soprattutto, da indirizzare in un campo specifico, che se pure nel vantaggio della specializzazione, ne limita il campo d'interesse.

Utili fonti sono anche le Università che con le loro continue ricerche scientifiche sono un enorme bacino d'informazioni precise e, soprattutto, attendibili.

Anzi, ci sono Università specializzate nella costruzioni di archivi e studi che allo stato attuale superano di gran lunga in qualità, quantità e competenza quelli delle agenzie governative di molti paesi.

Solo per fare alcuni esempi:

- l'Istituto di studi internazionali di Monterey ha la più completa banca dati mondiale sulla proliferazione delle armi nucleari, chimiche e biologiche;
- il Marcy Hurst College è specializzato sul traffico della droga;
- l'Università di Oxford ha creato un dipartimento chiamato *Oxford Analytica* che utilizza i docenti come un vero e proprio "Comitato d'Intelligence" in grado di fornire consulenze strategiche a livello mondiale (www.oxan.com, 2017).

4. L'analisi delle Informazioni

A questo punto il problema principale non sono le fonti quanto l'analisi delle informazioni.

È fondamentale la presenza di personale deputato a ciò che (come per l'Intelligence classica) deve essere particolarmente motivato e che abbia una cultura ampia e multidisciplinare, capace di non perdere mai di vista l'obiettivo e la mission delle informazioni in via di elaborazione.

La produzione d'Intelligence, perché sia davvero efficace, deve essere disponibile per il più ampio pubblico possibile senza compromettere la posizione politica dei fruitori, né quella dei vertici delle agenzie di Intelligence.

Con l'aumentare del livello di segretezza diminuisce drammaticamente, purtroppo, l'utilità dell'informazione.

Conoscere i segreti più nascosti del proprio nemico continua ad essere di fondamentale importanza per la sicurezza di ogni Nazione, ma è inutile correre rischi e affrontare costi elevati per raccogliere informazioni che potrebbe agevolmente recuperare anche uno studente.

Per sintetizzare: "In conclusione ogni Stato avrà ancora bisogno di spie e satelliti, che saranno utili solo all'interno di una comunità nazionale d'Intelligence in grado di utilizzare fonti aperte in modo rapido e a bassi costi" (Steele, 2002).

La prima tipologia di fonte aperta sono i media tradizionali: i mezzi di comunicazione di massa, la stampa sia nazionale che straniera, le televisioni, le radio e via dicendo.

Sistemi che offrono un'enorme quantità d'informazioni, ma non tutte utilizzabili ai fini dell'Intelligence.

I reportage e le inchieste giornalistiche sono generalmente gli strumenti più validi ed utilizzabili

quasi integralmente, in quanto connotati già originariamente come dossier.

Molto utili sono anche le pubblicazioni riconducibili a gruppi di appartenenza politica, parlamentare ed extraparlamentare, o gruppi organizzati di contestatori, come i *black bloc*, gli appartenenti ai centri sociali che sono soliti diffondere a mezzo Internet, come l'ormai chiuso *Indymedia*, opuscoli, volantini ed ogni sorta di idee e propositi di azione che non possono e non devono sfuggire alla disamina delle agenzie di Intelligence.

Non bisogna poi trascurare i libri di memorie e simili, che, se usati correttamente, possono fornire un valido strumento per il contrasto alle attività illecite.

Ne è un valido esempio il libro scritto da un capitano contrabbandiere inglese che operava nell'Adriatico negli anni cinquanta, trasportando tabacchi dal Montenegro all'Italia.

Il Comando generale della Guardia di Finanza ha tradotto il testo, pubblicato a Londra, da cui trasparivano le modalità operative dei contrabbandieri. Ciò permise di arrestare il traffico, con ingenti sequestri di beni e natanti (Meccariello,1994).

Anche il cinema può costituire una fonte aperta molto interessante per gli 007.

Il cinema non rispecchia solo la mentalità del regista, ma anche dei paesi produttori, rispecchiandone ideologia e cultura, tensioni, problemi e speranze.

Il cinema è soprattutto un fenomeno sociale. Ed in quanto tale descrive il mondo meglio di molti trattati e dossier.

Inoltre molti film sono stati scritti in collaborazione con la Cia ed altre agenzie di Intelligence, che in cambio di strumenti, di mezzi, e di un appoggio, inculcano nelle menti degli spettatori un'immagine di sé ben precisa.

Altra fonte aperta è Internet.

Va però sfatato il mito che vede in Internet la fonte attraverso cui l'Intelligence reperisce la gran parte delle proprie informazioni.

Il novanta percento delle informazioni utili non è neanche digitalizzato o pubblicato, ma è posseduto da compagnie o istituzioni private.

È pur vero però che il progressivo aumento degli utenti della rete e di Internet, la sempre maggiore pervasività nella vita delle imprese, istituzioni, gruppi e singoli individui, non consente di tralasciare questo strumento perché costituisce comunque un'importante fonte per l'Intelligence professionale, con riferimento all'aspetto tecnico-logistico.

Uno studio del 1994 effettuato dal *Community Open Source Program Office* (Cospo) della Nsc statunitense affermava che Internet contiene solamente quattrocentocinquanta siti veramente utili e comunque pieni di dati "grezzi", e che il novantanove percento dei contenuti della rete fossero pornografia, opinioni e pubblicità.

Gli esperti ritengono, infatti, che nel "web profondo" siano disponibili ad oggi duecentocinquantamila archivi potenzialmente utili per finalità d'Intelligence (NATO, 2001).

5. Conclusioni

A ulteriore riprova di quanto detto vi è un programma di sviluppo condotto dagli Stati Uniti che prevede un investimento finalizzato alla diffusione del computer nei paesi del Terzo Mondo per consentire l'accesso alla rete e facilitare in tal modo la possibilità di captare informazioni da parte dell'Intelligence statunitense.

Per la rete, infatti, circolano liberamente idee, informazioni ed anche propositi criminali.

È senza dubbio uno strumento mediatico capace di annullare le distanze ed abbattere barriere culturali e linguistiche fra organizzazioni religiose, politiche, sociali e criminali che possono utilizzare la rete per porre in atto differenti strategie di attacco e difesa, lecite ed illecite.

Le nuove tecnologie consentono d'inserire software in quasi ogni apparato elettrico, dai frigoriferi e lavastoviglie, alle automobili e telefonini, permettendo di tenere sotto controllo praticamente ogni cittadino del mondo civilizzato, conoscendone i gusti e le abitudini.

Una strategia dal nome chiaro, *pervasive computer*. Tecnologie che da un lato ci aiutano a vivere meglio e dall'altro ci rendono facilmente "detectabili".

Ciò è indubbiamente utile all'Intelligence economica.

Un frigorifero che si accorge che il latte sta per finire e che lo ordina direttamente al

minimarket di fiducia rivela quali sono i tuoi gusti e le tue abitudini, trasformandoti di fatto in una ricerca di mercato.

Internet comunque è sempre uno specchio sufficientemente attendibile della realtà con tutto ciò che di positivo e negativo comporta.

Alcuni studiosi della rete e dei fenomeni sociali ad essa connessi hanno notato come la struttura di Internet ha:

> *"il vantaggio aggiuntivo di poter condurre queste analisi utilizzando tecniche algoritmiche di navigazione e valutazione dei contenuti presenti. […] In un contesto come questo le organizzazioni reticolari risultano essere vincenti. […] Molte organizzazioni criminali e terroristiche che hanno adottato simili strutture con un sufficiente supporto di tecnologia Internet, hanno conseguito notevoli successi. Basti pensare alle attività di protezione e cripting delle informazioni di Al Qaeda che circolano in forma di posta elettronica tra cellule collegate; prima dei fatti dell'11 settembre fonti governative statunitensi hanno registrato un considerevole aumento di tale flusso informativo. Non c'è dubbio che queste nuove tecnologie stanno creando un problema nel campo della sicurezza, ma è altrettanto vero che le stesse tecnologie possono aiutare ad individuare soluzioni efficaci" (Corona, 2003).*

Utilissima anche la tecnologia dei motori di ricerca.

L'analista d'Intelligence uscendo dagli schemi accademici può trovare in strumenti come il *search engine* o il *data mining* due importanti alleati.

Sono strumenti in grado di ottimizzare i dati in una discriminazione ed interrelazione semantica d'informazioni apparentemente scollegate, con successiva catalogazione rapida delle informazioni discriminate.

> *"Tale metodologia è basata su alcune tecnologie note, come i motori di ricerca, nonché su nuovi algoritmi di acquisizione dei reticoli sociali tramite particolari spiders Internet, cui vanno aggiunti strumenti di analisi delle ontologie dei linguaggi per dati multilingua e catalogazione e clustering delle informazioni filtrate" (Corona, 2003).*

Inoltre le informazioni "crude" recepite comportano dei costi irrisori per i bilanci degli Stati; devono solo essere lavorate.

Altro esempio di "fonte aperta" è la "letteratura grigia" che include "documenti non convenzionali", come: audiovisivi, bollettini e newsletter, copioni teatrali, comunicati e rassegne stampa, cataloghi di mostre e traduzioni.

Data l'ampiezza della categoria, non esistono repertori esaustivi per l'individuazione dei riferimenti di tutta la "letteratura grigia" esistente, nemmeno a livello di Stati.

Alcune istituzioni e società private stanno creando delle banche dati settoriali, disponibili su Internet, informatizzando molti documenti o più spesso fornendo indicazioni bibliografiche.

Per esempio un progetto della comunità europea ha creato una banca dati denominata SIGLE (*System for Information on Grey Literature in Europe*), gestito dall'EAGLE (*European Association for Grey Literature Exploitation*), di cui fa parte per l'Italia il CNR, e disponibile a pagamento, online, o su Cd-Rom.

Nel novembre 2002 comprendeva circa 780 mila documenti (www.kb.nl, 2017).

Settore importante della letteratura grigia sono i *pre-print*, cioè la distribuzione delle pubblicazioni di ricerche, studi e teorie, molto tempo prima della loro apparizione nelle riviste scientifiche ufficiali, che prima di pubblicare un articolo lo sottopongono a un processo di controllo da parte di esperti internazionali.

Concludendo, i manuali ad uso interno delle agenzie di Intelligence, in particolare i manuali della CIA, sono le maggiori fonti per gli studi di settore.

Per quanto riguarda il criterio utilizzato nella raccolta di informazioni, i dati possono provenire da fonti riservate (dalla Difesa o altre agenzie di Intelligence), o da documenti Open Source come: archivi, pubblicazioni, radio, TV, giornali, dissertazioni scientifiche e fonti secondarie.

Le informazioni raccolte sono correlate a qualsiasi elemento ritenuto rilevante, sia una singola sezione di informazione o un elemento autonomo, purchè di comprovata affidabilità o facilmente verificabili (Colonna Vilasi, 2011).

Su di esso s'incentra per lo più l'attenzione delle unità di ricerca e di analisi.

I dati risultanti dal processo informativo sono spesso di grande importanza per la Sicurezza Nazionale.

Semplici, anche banali notizie, appropriatamente "lavorate" e inserite in uno scenario parzialmente abbozzato possono completare un'immagine, a volte molto rilevante.

References

Asker, J. R., (maggio 1994), *High-Resolution Imagery Seen as a Threat Opportunity*, in "Aviation Week and Space Technology".

Carapezza, E., Law, D. B., Stalker, K. T., (1999), *Unanttended Ground Sensor Technologies and Applications,* SPIE, Michigan.

Castelvecchi, A., Lo Re, C., Zardo, F., (2002), *L'Intelligence americana. Uomini, strutture e politiche dei servizi Usa*, Castelvecchi, Roma.

Colonna Vilasi, A., (2011), *Manuale d'Intelligence*, Città del Sole edizioni, Reggio Calabria.

Corona, G., (2003), *Network Analysis e Data Mining, nuove frontiere per l'Intelligence tecnologica,* in "per Aspera ad Veritatem", n. 26.

Eftimiades, N., (1994), *Chinese Intelligence Operations*, Naval Institute Press, Annapolis.

Gagliano, G., (2011), *Problemi e prospettive della Intelligence del XXI secolo,* Editrice UNI Service, Milano.

Izzi, S., (2011), *Intelligence e gestione delle informazioni. Attività preventiva contro i traffici illeciti*, Franco Angeli, Milano.

Johnson, L. K., (2006), *Strategic intelligence,* Greenwood Publishing Group, Westport.

Johnson, L. K., (2000), *Per le spie c'è ancora molto lavoro*, in "Global FP", n. 5.

Kock, W. U. (a cura di), (2011), *Counterterrorism and Open Source Intelligence,* Springer, Odense.

Lowenthal M. M., (2017), *Intelligence. From Secrets to Policy*, Seventh Edition, CQ Press, Thousand Oaks, California.

Marcevski, A., (2002), *Misteri italo-bulgari,* Stango, Roma.

Meccariello, P., (1994), *Finanza di mare dalle scorridore ai pattugliatori*, Editalia, Roma.

Messina, P., (2012), *Il cuore nero dei servizi,* RCS, Milano.

NATO, (2001), *Osint handbook*, Saclant, Norfolk (VA).

Phythian M., (2013), *Understanding the Intelligence Cycle*, Routledge, London.

Quigging, T., (2007), *Seeing the Invisible: National Security Intelligence in an Uncertain Age*, Qorld Scientific, London.

Rapetto, U., Di Nunzio, R., (2002), *L'Atlante delle spie: dall'antichità al grande gioco a oggi*, Rizzoli, Milano.

SCUOLA DI GUERRA-COMANDO C4IEW, (1999), *Manuale S2/G2*, Roma.

Steele, R. D., (2002), *Intelligence. Spie e segreti in un mondo aperto,* Rubettino, Soveria Mannelli.

U.S. MARINE CORPS, (2007), *Counterintelligence,* Cosimo, New York.

Website

http://www.kb.nl (August 8, 2017)

http://www.sicurezzanazionale.gov.it/web.nsf/pagine/glossario-intelligence (January 13, 2017)

http://www.oxan.com (March 26, 2017)