LUISS Guido Carli
LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

Dipartimento di Scienze Politiche

Cattedra di Sociologia della comunicazione

Intelligence e New media, tra Segreto di Stato e trasparenza globale

RELATORE

Prof. Michele Sorice

CANDIDATO

Rebecca Mieli

Matr. 068252

Anno Accademico 2014/2015

Intelligence e New media, tra segreto di stato e trasparenza globale

INDICE

Capitolo I

L'informazione diventa comunicazione: evoluzione da spionaggio a Intelligence

Spionaggio Informativo e Intelligence Comunicativa 3

Ragion di Stato e stabilità istituzionale nell'occidente democratico 5

Non più Spie di guerra, ma analisti di mercato 7

Capitolo II

Intelligence e New Media, armi a doppio taglio del mondo globalizzato

Ricerca, fonti e analisi: processi di elaborazione dell'Informazione 10

New Intelligence: Gestire la conoscenza a livello globale 11

L'importanza dell'informazione nel mondo di oggi 13

Capitolo III

Open Source Intelligence e Cyber Intelligence: Inquinare le informazioni servendosi dei media.

Penetrazione nel circuito Informativo: Disinformazione e guerre semantiche 17

Open Source Intelligence, la nuova sfida globale 19

Cyber Intelligence: il world wide web al servizio dei decisori 21

Capitolo IV

Case Studies, confronto tra Italia, Unione Europea e Comunità Internazionale

Fallimento delL'Intelligence nel Decennio Breve: 9/11, Madrid, Londra 24

WikiLeaks, il Quinto Potere contro il Segreto di Stato 27

Datagate: Privacy, riservatezza, sicurezza. 28

Conclusione 31

Capitolo primo – L'informazione diventa comunicazione: evoluzione da spionaggio a Intelligence

Spionaggio Informativo e Intelligence Comunicativa

Il concetto di "spionaggio" così come il concetto di "mezzo di comunicazione", appartengono a quella categoria di eroi incompresi della società, moderna certo, ma anche antica. Eroi incompresi quindi, quelli che dividono l'opinione pubblica a metà tra chi crede che stiano uccidendo la società e chi crede che la stiano solo facendo progredire più velocemente di quanto non avrebbe fatto da sola. Chiamarli Intelligence e New Media non cambia la situazione di equilibrio precario in cui si trovano, tra la ragione e il torto, tra il bene e il male. Raccogliere dati segreti o sconosciuti è il fulcro dell'attività di spionaggio, ma senza dubbio lo è anche della comunicazione, soprattutto dal momento in cui la Einkommende Zeitungen[1] varcò i cancelli della storia. L'epigrafe di Simonide alle Termopili è uno dei primi esempi a noi pervenuti del fatto che "la comunicazione di massa esiste da sempre" (Balassone, 2, sd) è che è sufficiente che un messaggio si rivolga a una vasta quantità di soggetti sconosciuti ed indeterminati per essere inserito nella citata categoria. Per parlare di spionaggio, invece, è necessario che il messaggio sia segreto, e che venga diffuso proprio ai soggetti per cui il segreto era stato creato, coloro che sarebbero dovuti rimanerne all'oscuro. Questa pratica viene fatta risalire comunemente alle origini delle prime popolazioni, poiché considerata merce di vitale importanza per la difesa della propria gente: Sumeri, Egizi, Ebrei, Fenici, Assiri, Romani e Persiani si sono probabilmente serviti dell'attività di spionaggio in campo militare, anzi, l'argomento era certo considerato un tabu in misura assai minore di quanto non lo sia oggi. Percorrendo la storia, troviamo esempi di spionaggio anche nella Repubblica di Venezia, nel Giappone Feudale e nell'Inghilterra Vittoriana. Tutto il mondo, tutte le epoche, tutti hanno visto popoli e nazioni intere giocare sporco contro i propri nemici. Certo la parabola non finisce qua, poiché molto possiamo dire dei numerosi e controversi casi di tradimenti perpetrati da normali cittadini contro il loro stesso paese. Il generale americano Benedict Arnold è l'esempio di come gli interessi del singolo prevalgano sempre su

[1] Trattasi del primo quotidiano della storia, pubblicato a Lipsia nel 1660.

qualsiasi tipo di giuramento. In ogni caso, tutti i maggiori studiosi di Intelligence sono d'accordo nel definire la prima metà del novecento come l'epoca d'oro dello spionaggio, frutto ovviamente della loro estrema utilità negli infuocati anni delle due guerre. Un esempio potrebbe essere sintetizzato nella decodifica dei codici cifrati Giapponesi durante la Secondo Guerra Mondiale da parte degli Stati Uniti, la quale eliminò il rischio di alcuni attacchi aerei contro la flotta americana, oppure la stretta rete dei servizi segreti russi che riuscì a bloccare i rifornimenti tedeschi spianando la strada verso la disfatta di Stalingrado. Chiaramente con la nascita del Diritto Internazionale e dell'era della Globalizzazione la figura della spia è andata ad assumere sempre di più un ruolo negativo, come un complottista che definisce rivali o nemici, nazioni che, se non chiaramente amiche, risultano essere probabilmente alleate, specialmente in campo economico. Lo sviluppo "biologico" dello spionaggio, che Alessandro Ceci chiama "Ontogenesi" (Ceci, 2007), avviene quasi totalmente dopo la Guerra Fredda, nel momento in cui spiare diventa *Inter-legere*, ossia leggere dentro. Per comprendere meglio il significato di queste due locuzioni basta tornare a parlare di mezzi di comunicazione di massa, e del momento in cui sono diventati veri e propri "new media". Lo sviluppo delle nuove tecnologie ha trasformato l'informazione, intesa come la formulazione di un messaggio indirizzato ad uno o più destinatari, in comunicazione, nella quale troviamo un elemento fondamentale e quanto mai caratteristico dell'era in cui viviamo: il feedback. Nello schema tradizionale composto da emittente e ricevente, dove il primo invia un messaggio al secondo attraverso un canale di trasmissione, il feedback si colloca infondo, alla fine del percorso, e indica la risposta del ricevente al messaggio. Non c'è una data in cui possiamo dare per certo che l'informazione sia diventata comunicazione, ma è certo che molto dipende dalle tecnologie, dalla possibilità di controllare gli indici d'ascolto in un primo momento, fino ai nuovi fenomeni di Citizen Journalism e User Generated Content. Se l'era 2.0 ha portato la comunicazione ad essere un frutto della condivisione tra fruitori più attivi che mai, la medesima rivoluzione è avvenuta per l'Intelligence, che da Intelligence dell'informazione è diventata della comunicazione, anzi, risulta essere vera e propria *azione comunicativa* (Ceci, 2007). Analizzando questo cambiamento appare chiara la differenza nell'approccio al corpo dei servizi segreti tra le varie

nazioni. Israele e Italia sembrano aver compiuto al meglio questo passaggio; ne è la prova il fatto che l'azione comunicativa vera e propria si integra ad una continua relazione con l'esterno. Mentre la CIA e la NSA tentano di costruire una difesa nazionale unicamente sulla base delle proprie forze, il Mossad sembra agire in maniera opposta, cercando e recuperando documenti segreti, ma parallelamente costruendo una rete di collaborazione con altre agenzie di Intelligence; inoltre sono gli unici ad adottare un sistema non bipolare, applicando la medesima politica di sicurezza verso tutti, senza differenza tra alleati e non. Alessandro Ceci fornisce un esempio ancora più concreto: tre formiche, situate una di fronte ad un elefante, una alla sua destra e una dietro di lui, osservano l'animale. É chiaro che ognuna di loro nonostante la vicinanza, abbia solo una visione parziale dell'animale, e ne fornisce una propria interpretazione, ma se le formiche lavorassero insieme, collaborando per costruire un'informazione unica? Il risultato sarebbe quello di avere una visione d'insieme dell'animale, una conoscenza certamente più completa anche se inizialmente frazionata. Le formiche rappresentano L'Intelligence strategica che guarda i fenomeni cosi come avvengono, L'Intelligence operativa, che studia i retroscena e l'organizzazione che hanno alle spalle, infine L'Intelligence investigativa, che li guarda da dentro. L'obiettivo è ancora connesso alla sicurezza, ma con queste premesse si discosta dal essere solo uno strumento nelle mani del potere, diventando una forma di protezione dell'intera nazione, del popolo e della democrazia.

Ragion di Stato e stabilità istituzionale nell'occidente democratico

Non ho usato il termine Democrazia a caso: quando il potere è legittimato dal popolo, la legge diventa uno strumento di promozione dell'uguaglianza. Se la legge è uguale per tutti, perché un qualsiasi dipendente di un'agenzia di Intelligence può agire illegalmente? In realtà si tratta, nel caso specifico, di azioni extra giuridiche. Ma come convincere, o meglio convincersi, che la scelta di spiare i propri nemici o chi si pensa che possa trasformarsi in un nemico, sia in qualche modo etico? Fino a che punto la privacy può essere calpestata dalla famosa ragion di stato? In questo caso è opportuno analizzare la democrazia in cui viviamo. La democrazia odierna si basa, come già detto, sulla comunicazione, in essa nasce e senza di essa non

potrebbe prosperare. Che la comunicazione fosse la base della democrazia, lo avevano già specificato Popper e, ancora prima, Socrate. Ovviamente sembravano essere semplicemente teorie, ma oggi che la tecnologia ci permette di vivere nell'era della comunicazione, ci sembra quasi che abbiano detto una ovvietà; non altrettanto ovvio era il potere che avrebbero preso i media, i quali oggi sono considerati l'unica fonte di legittimazione dei leaders. Ora ci si chiede, in un mondo democratico in cui tutto sembra essere regolato da fredde e dure leggi a garanzia della pace, a che serve L'Intelligence? Si sono attenuati i conflitti tra stato e stato, quelli esterni, ma sono fiorite nuove minacce, prima su tutte quella del *terrorismo,* una minaccia ben peggiore di qualsiasi guerra tra eserciti, perché nascendo nell'ombra, non ha potere, e per questo vuole conquistare notorietà e visibilità, essere legittimata come forza sovversiva con gesta clamorose, e per clamorose intendo ricche di vittime innocenti. Il potere, inteso come la capacità di guidare una nazione nel suo stesso interesse, non è più al centro della scena; il *balance of power* o il nazionalismo non guidano la nostra società ormai da mezzo secolo. La visibilità è l'unica cosa che può rendere più potente un'organizzazione terroristica senza volto rispetto a un'organizzazione internazionale nata per garantire la sicurezza di tutti. Ed è la visibilità che cercano anche le agenzie di Intelligence per sentirsi legittimate a combattere una battaglia contro queste nuove minacce, studiando i comportamenti ricorrenti delle popolazioni per individuare dei segnali che, seppur immergessi in realtà democratiche, indicano chiaramente la volontà di colpirla nel profondo. Non si può comprendere il ruolo dell'Intelligence nell'era della comunicazione senza analizzare a fondo il nemico contro cui combatte. La comunicazione, afferma Ceci riprendendo McLuhan, porta alla luce i concetti di *pieno* e *vuoto,* dove si potrebbe legare al primo, la minaccia di una nazione che ne attacca un'altra per conquistarla, e al secondo la minaccia terroristica. Lo scopo di un attentato non si può ridurre alla semplice produzione di terrore, ma al garantire un sentimento di vuoto dentro alle popolazioni colpite, come la percezione che né la legge né le istituzioni possono salvarli, un fenomeno che genera null'altro che insicurezza e sfiducia nel mondo democratico. L'insicurezza porta al distacco dal proprio paese e dei propri leader, e piano piano, erodendo questo sentimento, l'uomo si ritrova ad essere esattamente come il terrorista, senza nome e senza

identità, insicuro e abbandonato, senza più connessione con la propria cultura e con la propria storia, giorno dopo giorno meno fiducioso nella democrazia. Risultano chiare, a questo punto, due grandi verità: in primis, il potere politico, da solo, non può garantire la sicurezza dei cittadini; in secondo luogo quando il cittadino non si sente al sicuro, tende a volersi difendere da solo, il che, nella maggior parte dei casi, risulta essere uno scavalcamento delle leggi e delle istituzioni. Ceci da un esempio di questa seconda teoria: Un ragazzo terrorizzato dall'idea di prendere un volo s'informa, presso una società di assicurazioni, circa le probabilità che sull'aereo che deve prendere possa esserci una bomba. Gli viene risposto una su centomila, ma non sentendosi ancora tranquillo chiede se la probabilità che le bombe siano due corrisponda ad un numero ancora più basso. Gli viene risposto, probabilmente uno fratto il quadrato di centomila, una probabilità quasi inesistente. Poco tempo dopo, il giovane venne arrestato nel tentativo di salire sull'aereo con una bomba, gesto compiuto nella speranza di diminuire il rischio che ve ne fosse un'altra. Forse, fatte queste premesse, L'Intelligence di oggi può aiutare la popolazione a sentirsi più sicura senza allontanarsi necessariamente dalle istituzioni democratiche.

Non più Spie di guerra, ma analisti di mercato

Sun Tzu, né "l'arte della guerra" definisce cinque tipi di spie: locali o civili, interne, cioè infiltrate tra le linee nemiche, doppie, cioè coloro che facevano parte dello spionaggio nemico, morte o vive a seconda che fornissero informazioni false o vere (Ceci, 2007). Un sistema antico eppure paradossalmente così moderno da riuscire a funzionare per centinaia di anni, per lo meno fino alla fine degli anni ottanta. Lo sviluppo dell'Intelligence comunicativa si è concretizzato nella richiesta di un gran numero di analisti, quasi come se la figura della spia avesse perso la sua importanza, similmente è avvenuto per la figura storica del giornalista, considerata per due secoli la "voce della verità" e oggi sostituito da data journalists, più *geeks* esperti di informatica che vere e proprie "penne". Analisti, dunque, che scompongano fenomeni come il terrorismo e la criminalità organizzata, con

l'obiettivo di tutelare lo stato anche se questo possa significare la regressione del processo democratico. In un contesto come questo, in cui abbiamo già chiarito l'extragiuridicità e il leggero allontanamento dalla democrazia che può essere considerata una diretta conseguenza della parte più occulta dell'attività di Intelligence, il cambiamento dell'approccio alla sicurezza si sta trasformando in qualcosa di più marcatamente *pubblico* e trasparente, ad esempio il caso dei servizi segreti britannici, che in tempi recenti hanno reclutato nuovi impiegati su facebook tramite un annuncio che recitava "Time for a career change? MI6 can use your skills!". Questa parabola "evoluzionistica" appena tracciata circa l'approccio comunicativo dei servizi segreti potrebbe cambiare per sempre il ruolo di questi all'interno della società occidentale e concretizzarsi in un vero e proprio veicolo di modernizzazione. Ma come funzionano i servizi segreti? L'Intelligence di oggi, che ancora una volta vogliamo definire Intelligence Comunicativa ha come obiettivo quello di difendere la sicurezza dei cittadini, contrastando tutte le varie minacce alla sicurezza territoriale, alla stabilità dei governi o comunque agli interessi della nazione. Si può scomporre l'attività di Intelligence in otto principali fasi: incarico, raccolta, valutazione, classificazione, collazione, analisi, previsione, divulgazione (Colonna Vilasi, 2011). L'Intelligence è strettamente connessa alle relazioni internazionali, ai rapporti di forza ma anche al mercato globale; questo perché nonostante l'occidente si trovi in un periodo storico di pace, le nazioni si trovano in un momento di *vulnerabilità condivisa* (Ceci, 2007) in cui la concorrenza economica sembra definire una spaccatura sempre maggiore tra paesi ricchi e paesi poveri, come una nuova guerra più psicologica che fisica, combattuta tra PIL e PNL, e che proprio come una guerra richiede una forma di Intelligence tutta dedicata ad essa. Inoltre una parte sostanziale di essa non si limita all'attività informativa offensiva e difensiva[2], ad esempio una fetta non piccola si occupa dell'intossicazione, ossia di fornire false notizie ai nemici o anche di influenzare i vertici e il popolo attraverso la manipolazione mediatica. Insomma Media e Intelligence sono due satelliti dello stesso pianeta, il gigantesco pianeta della Democrazia Comunicativa: il primo nato per comunicare l'alto messaggio dei

[2] L'attività informativa delL'Intelligence si divide in offensiva, cioè raccolta di dati altrimenti segreti, o difensiva, cioè salvaguardia delle proprie informazioni (Colonna Vilasi,2011).

leaders verso la bassa e mal istruita popolazione, si ritrova a comunicare per vie orizzontali, mentre il secondo, nato per difendere il basso popolo dall'oppressione dell'alto esercito nemico, oggi tenta di difendere le alte istituzioni e la sovranità dei poteri, dalla bassa e nascosta minaccia del terrorismo.

Capitolo secondo – Intelligence e New Media, armi a doppio taglio del mondo globalizzato

Ricerca, fonti e analisi: processi di elaborazione dell'Informazione

"Il processo informativo può essere inteso come la successione delle attività concettuali, organizzative ed esecutive attraverso le quali si perviene agli elementi necessari per la conoscenza dell'avversario" (Colonna Vilasi, 2011, 44). La ricerca, ovvero la prima fase, si svolge analizzando gli elementi essenziali dell'informazione che perviene dall'analisi del comportamento del soggetto studiato, nello specifico un avversario. Questi elementi vengono raccolti e classificati, esaminandone il livello d'interesse che il grado di attendibilità, i quali risultano essere dei criteri oltremodo spinosi , richiedenti un'enorme quantità di tempo ed energie. Attribuito, in conformità a questi criteri, un valore alla notizia, si passa all'attività d'integrazione, la quale consiste nel coordinare la notizia appresa con le altre già classificate. Le fonti[3] sono particolarmente importanti. In particolare, quando si parla di Intelligence, le fonti vengono tendenzialmente ripartite tra fonti "umane" (HUMINT), nel senso di veri e propri informatori diretti, e gli strumenti tecnologici (SIGINT). Nei giorni nostri una nuova, potentissima fonte si appresta a connettere le prime due, unendole ma scavalcandone l'importanza con facilità, la *Open Source Intelligence (OSINT).* Tutte e tre meritano una spiegazione più approfondita: la HUMINT rappresenta la datata concezione di spionaggio come raccolta di informazioni in prima persona, una raccolta segreta e quindi risalente alla vecchia concezione di Intelligence Informativa. La SIGINT è legata alla moderna tecnologia informativa e si serve, ad esempio, di rilevamenti satellitari e segnali radar o sonar. La OSINT è il diretto risultato della nuova società mediatica e trasparente; si basa su documenti come dispacci, testi di interrogatori, lettere, documenti cartacei e online che possono essere reperiti da chiunque, risultando proprio per questo cosi complessi, perché necessitano di uno studio approfondito su quelli che sono i gradi di veridicità e di rilevanza dell'informazione che diffondono. Essendo L'OSINT definita come *"l'attività di raccolta di informazioni mediante la consultazione di fonti di pubblico accesso" (Wikipedia)* al primo posto tra le varie fonti ci sono i

[3] Antonella Colonna Vilasi le divide in controllate, non controllate, aperte o casuali

nuovi media. Reportage ed Inchiesta, Data Journalism[4] e Citizen Journalism[5], cinema e letteratura sono tutte preziose fonti utilizzate dall'Intelligence Comunicativa specializzata nell'Open Source. Internet si rivela essere terreno fertile non solo per idee e contenuti personali, ma è a tutti gli effetti la rete più utilizzata da criminali e terroristi, ad esempio può essere un sito web pedopornografico, o le attività di cripting delle informazioni inviate da Al Quaeda. Ulteriori strumenti come il *Web Search Engine* (ovvero i motori di ricerca) o il *Data Mining*[6] sono incredibilmente preziosi nonostante il costo pari a zero. Una volta classificate le fonti si può passare alla fase della *distillazione,* in cui si scompongono i dati e si estrae solamente il contenuto davvero rilevante, e *l'analisi informativa*, che consente di determinare il valore di una notizia su una scala di sei gradi di valore. Per quanto riguarda la fase analitica, essa non dovrebbe in nessun caso essere svolta da un computer, ma necessita di un'equipe di esperti analisti, soprattutto delle discipline psicologiche e logico-cognitive (Colonna Vilasi, 2011).

New Intelligence: Gestire la conoscenza a livello globale

La storia dello spionaggio ha invertito la sua rotta quando il mondo bipolare, conteso come ad un tiro alla fune tra Stati Uniti ed Unione Sovietica , ha lasciato spazio alla caduta del muro di Berlino, alla fine dell'URSS, e quindi alla completa egemonia Statunitense. La preponderanza della nazione a stelle e strisce può considerarsi sia come mondo unipolare, in quanto era considerata come l'unica vera potenza mondiale, o come passaggio dal bipolarismo a multipolarismo, perché ha lasciato spazio non solo alle altre nazioni che smisero di sentire la tensione del conflitto ma anche perché ha dato modo a minacce extranazionali (prima su tutte il terrorismo), di aumentare la propria influenza. La minaccia militare si è ridotta a zero, sostituita da quella economica che si è ritrovata ad assorbire le attenzioni delle potenze emergenti. "Venendo a mancare uno dei due blocchi, il sistema ha perso la capacità di autoregolazione. Liberando cosi le mire dei singoli stati che

[4] Approccio giornalistico che fa uso di database, software e dati statistici digitali.
[5] Giornalismo partecipativo, svolto da persone comuni registrando una notizia con uno smartphone o comunque documentando un fatto dal luogo stesso in cui avviene tramite fotografie e video.
[6] Il ***data mining*** è l'insieme di tecniche e metodologie che hanno per oggetto l'estrazione di un sapere o di una conoscenza a partire da grandi quantità di dati (attraverso metodi automatici o semi-automatici) e l'utilizzo scientifico, industriale o operativo di questo sapere. (Wikipedia)

hanno ripreso a ragionare in termini d'interessi nazionali, di geopolitica e di potenza" (Colonna Vilasi, 2011, 78). L'Intelligence è stata, dunque, costretta a diramarsi verso due direzioni: una parte si è avvicinata alle multinazionali ed in generale alle aziende per affrontare la nuova sfida economica (soft power), parallelamente le agenzie di Intelligence legate alla politica internazionale si sono attrezzate per combattere nuovi tipi di minacce, degli scontri etnici della ex Jugoslavia alla Jihad Islamica (hard power). Quest'ultima è sempre più dipendente dalla tecnologia: in primo luogo perché viviamo in un mondo in cui i diritti umani sono messi al primo posto, di conseguenza si cerca di coinvolgere il meno possibile l'elemento umano in combattimento, e in secondo luogo perché la trasparenza della globalizzazione ha aumentato il flusso quotidiano delle informazioni, da cui prima non si attingeva con tanta facilità. Anche la forza, da sempre misurata sulla base del quantitativo e della potenza delle armi possedute, inizia ad essere misurata con altri criteri, come il livello di acquisizione ed il livello di gestione delle informazioni ottenute. L'Intelligence sta combattendo le guerre come un vero e proprio esercito, basandosi più di tutto sulle risorse economiche e sull'acquisizione di tecnologie esclusive. Ovviamente questo cambiamento non è tutto rose e fiori, gli Stati Uniti sono spesso accusati di utilizzare troppa tecnologia, anche in quelle fasi del processo informativo dove si necessita l'intervento umano, e per questo si parla spesso dell'11 Settembre come il fallimento dell'Intelligence americana. La critica deriva dal fatto che la mancanza delle fonti aperte negli anni più caldi della guerra fredda ha portato la CIA, l'FBI la NSA e la DIA a concentrarsi sulla ricerca delle informazioni; oggi le fonti aperte permettono di disporre di una vasta gamma di informazioni, la difficoltà passa alle fasi di selezione ed analisi in cui L'Intelligence europea e quella israeliana sembrano avere la meglio. I conflitti di tipo etnico-religioso iniziano, peraltro, sia ad influenzare pesantemente l'opinione pubblica internazionale, sia ad esserne influenzati; i fondamentalismi e gli estremismi nascono nella globalizzazione proprio per sfuggire alla fascia d'influenza occidentalizzante. Questa nuova minaccia necessita di un ritorno alla HUMINT, in quanto la tecnologia che ci ha sovrastati non permette più di distinguere con facilità tra la notizia vera e quella falsa, e inoltre gli manca la capacità analitica tipica di una "spia" degli anni cinquanta. L'Open Source

Intelligence dunque può essere un valido strumento per le agenzie di Intelligence e per le nazioni in generale, ma non deve però lasciare indietro la risorsa umana, che nel campo dell'analisi fatica a trovare una macchina in grado di sostituirla. L'OSINT riduce i costi e il livello di segretezza delle operazione di Intelligence, è eticamente inattaccabile, come invece sembra essere la classica definizione di spionaggio, non limita in alcun modo il diritto alla conoscenza del cittadino, in quanto fa uso di mezzi di comunicazione e di informazione aperti a tutti e può essere un valido strumento per combattere l'Information Warfare, espressione coniata da Robert David Steele che esporrò più avanti. Insomma, si parla molto di sicurezza governativa, ma gestire la conoscenza a livello globale con questi nuovi strumenti è la rampa di lancio verso una nuova funzione delL'Intelligence, cioè la difesa degli interessi della collettività.

L'importanza dell'informazione nel mondo di oggi

Per comprendere al meglio il ruolo che i servizi segreti svolgono nei confronti dell'industria mediatica è necessario fare una panoramica sul ruolo dell'informazione ai nostri giorni. In particolare le affinità tra le due cose andrebbero analizzate con il "microscopio" in quanto elementi come la notizia, la fonte, lo scandalo e la fonte aperta (solo per citare alcuni esempi) si rivelano appartenere sia al sistema di Intelligence sia a quello mediatico, di conseguenza prima di passare all'interazione tra i due sistemi, è giusto capire come funzionano i media dell'era 2.0. In primis il rapporto tra servizi di informazione e mezzi di informazione dovrebbe collocarsi tra gli studi politici e gli studi economici, ovviamente molto più spesso si parla dei secondi, questo sia perché viviamo nell'era della produzione continua di dati e notizie, sia perché il consumo e quindi il mercato dei media è forse uno dei più fiorenti al mondo. Le scienze sociali nei paesi anglosassoni, sono solite trattare ampiamente anche la tematica dei servizi segreti, mentre dall'altro lato, nel continente e specialmente in Italia, questi aspetti vengono lasciati in disparte proprio perché non si ama trattare gli aspetti più "dark" della società. Si possono dare sostanzialmente due letture differenti in merito al rapporto tra Intelligence e New Media, in primis la manipolazione, cioè quell'aspetto che si occupa della produzione dell'Informazione e come questa

venga, appunto, manipolata dall'Intelligence. La seconda è il consumo, ad esempio come i servizi segreti attingono dalle fonti aperte per costruire una rete informativa. In generale appare evidente che un improvviso default del sistema informatico potrebbe distruggere la nostra società, che si ritrova catapultata in una relazione di netta dipendenza dal sistema delle comunicazioni. Tutto ciò porta ad affermare con certezza la centralità dell'Intelligence come garante della sicurezza della società, perché viene in assoluto usata come principale arma di difesa del sistema informativo. Fatte queste premesse la relazione di interdipendenza appare chiara. Quale dei due mezzi sia più "potente" appare ancora più chiaro, nonostante si regga sulla protezione fornita dall'altro. Qualcosa c'è di più forte, che se possibile manipola entrambe, ed è la figura del "decisore", identificata con lo Stato, o come chi detiene il potere in una società. Quindi l'elemento decisionale non è di competenza né dell'uno né dell'altro, ma dello stesso soggetto che decide per entrambi. Come si formano le notizie? Il primo elemento, sia per importanza che per successione temporale è la fonte. Le fonti possono essere ufficiali e ufficiose, le prime sono comunicati e conferenze, il cui scopo è far conoscere la novità, mentre le fonti ufficiose sono sostanzialmente confidenze e informazioni estratte nei rapporti tra privati. Spesso, ad esempio, le fonti vogliono restare anonime, ed è un dovere di giornalista rispettare questa volontà. Quest'ultime possono classificarsi ulteriormente in fisse o occasionali, tenendo sempre presente che le informazioni che possono derivare da una fonte fissa (spesso e volentieri pagata profumatamente) sono sicuramente professionali ma influenzate dagli interessi privati del soggetto, mentre le fonti occasionali sono un genere più grezzo ma più genuino. Di qualsiasi tipo siano le fonti, la maggior parte non è verificabile dal comune fruitore di un giornale o di un servizio televisivo, e anche quando lo è, le persone che si sincerano della veridicità di una notizia perdendoci del tempo sono certamente una minoranza. Qui entra il gioco la credibilità del giornalista come elemento portante della visibilità della notizia. Un altro elemento di fondamentale importanza, specialmente per L'Intelligence, è l'agenzia di stampa, dal quale i giornalisti attingono ma che è stata negli anni influenzata da quest'ultima allo scopo di diffondere più velocemente una notizia, o viceversa di occultarne un'altra. Ovviamente anche quando le notizie vengono date dall'agenzia stampa, è difficile

avere la certezza che ogni pezzo riportato corrisponda ai fatti, in questo senso il giornalista molto più dell'agenzia stampa, possiede l'arma del linguaggio, ad esempio l'utilizzo del condizionale invece che dell'indicativo. Il linguaggio è anche indispensabile per fare presa sul pubblico, per esempio un linguaggio più tecnico come quello dei quotidiani economici rende il tutto comprensibile solo da una minoranza di esperti. Il lavoro del giornalista quindi è fare uso delle notizie fornite dall'agenzia stampa per dare una propria interpretazione dei fatti. Ma non è solo questo: l'attività di ricerca svolta quando si sta facendo un'inchiesta è chiaramente più pura ed incontaminata. indipendente dal tempo e derivata dalle sole fonti primarie, l'inchiesta richiede una ricerca di spessore, meglio se incentrata su una tematica poco trattata e che possa simboleggiare un vero e proprio studio scientifico. Per quanto riguarda invece la struttura del giornale, lo schema risulta essere abbastanza libero: l'editore ed il direttore possono scegliere quali notizie mettere in prima pagina e quali no, l'importante è che si rispettino alcune semplici regole, come l'inserimento della testata in cima o la spalla accanto all'articolo di fondo. L'impaginazione non è un elemento da sottovalutare, perché può influire sulle opinioni del lettore quasi quanto una opinione faziosa malcelata. Umberto Eco, sul numero de "l'Espresso" del Luglio 1969 parla del giornale come uno strumento manipolatorio e molto potente che influisce sui lettori anche quando il testo dell'articolo risulta oggettivo. L'impaginazione, la scelta delle notizie, la gerarchia degli articoli, le immagini, i titoli, sono il frutto di un'informazione che non può materialmente rivelarsi oggettiva. Anche il giornalismo anglosassone, che è sempre stato annoverato come un "quarto potere" distante dagli altri, e che mira da quasi duecento anni alla separazione tra i fatti e le opinioni, non può considerarsi completamente oggettivo. Per quanto riguarda il giornalismo continentale, la faziosità viene quasi messa in risalto, in quanto i giornali nacquero quasi ovunque con lo scopo di sostenere un partito o una classe politica o lavoratrice. Per Ottone (Si parla quindi di dibattito tra Eco e Ottone) l'oggettività, o meglio la mancata oggettività dei giornali non può considerarsi una colonna portante, perché diventerebbe un alibi per non informarsi. Questa è l'ipotesi maggiormente avallata da Aldo Giannuli (2012) nel senso che sebbene "ricostruzioni tendenziose" tendano a manipolare l'opinione pubblica, anche da

queste possiamo estrarre validi contenuti, sia perché si presuppone sempre la professionalità del giornalista, sia perché l'effetto distorsivo si riduce proporzionalmente all'aumento della consapevolezza del lettore, e sia perché le distorsioni fornite da più network informativi vengono a compensarsi l'un l'altro. L'attore più importante ed influente che si muove sul palcoscenico del mondo dell'informazione è forse l'editore. L'editoria è "l'attività imprenditoriale di produzione e gestione di contenuti riproducibili in serie e della loro diffusione e commercializzazione in forme trasmissibili attraverso i media" (Wikipedia). L'editore definisce l'orientamento del giornale, ed è anche quella posizione che più si avvicina ai servizi di Intelligence in quanto diventa quasi "gli occhi e le orecchie" del giornale. Il lavoro dell'editore deve basarsi sull'imprenditorialità, non sul "saper scrivere", la base di questo lavoro è il salotto, le buone conoscenze il saper trarre notizie di interesse anche a partire da una chiacchierata informale in cui si possono inserire indizi come tasselli di un puzzle. Questa è una forte similitudine con l'attività di Intelligence perché ci si ritrova a estrapolare un'informazione anche da frasi o comportamenti che agli occhi di chiunque altro sembrerebbero irrilevanti. Oltre all'editore abbiamo, su scala gerarchica, il direttore, il caporedattore, i capiservizio e i redattori semplici. Giannuli (2012) paragona il giornalista, che chiama "Public relations man" alla figura dello Spin Doctor, il quale elabora strategie di immagine e di comunicazione per conto di uomini di potere, e che opera contrastando l'informazione avversaria condizionando l'opinione pubblica. Un ultimo fondamentale appunto sul legame tra new media e Intelligence è il controgiornalismo, quindi quell'attività giornalistica antisistema che si sta sviluppando ogni giorno di più sul web, non esposta al costante controllo statale, libera dai formalismi che stanziano nelle sale del potere, ma soprattutto messa in piedi dai giovani collegati da una rete comunicativa decisamente più solida di quella cartacea. Il controgiornalismo viene paragonato al controspionaggio, nato molto prima ma che certamente risente oggi più che mai l'influenza della tecnologia mediatica 2.0.

Capitolo terzo – Open Source Intelligence e Cyber Intelligence: Inquinare le informazioni servendosi dei new media.

Penetrazione nel circuito Informativo: Disinformazione e guerre semantiche

Lo scopo dei Servizi d'Informazione è, come abbiamo già detto, la tutela degli interessi stateli, in particolar modo L'Intelligence svolge attività offensiva, quando tenta di reperire informazioni dall'esterno e difensiva, nell'atto di proteggere le proprie. La penetrazione che questa ha iniziato a svolgere nel circuito informativo pubblico non è altro che mera, e a questo punto prevedibile, manipolazione della realtà circostante. La facilità con cui questo processo è posto in essere viene soprattutto dal fatto che sia i servizi sia i mezzi d'informazione svolgono un'attività retribuita, controllata e in generale gestita dai decisori, i quali hanno a disposizione apparati di raccolta, produzione e analisi delle informazioni. Come può svolgersi un'attività di penetrazione all'interno di un apparato mediatico? Solitamente con l'Infiltrazione diretta, ad esempio un'assunzione pilotata, tramite ricatti o più semplicemente tramite uno scambio, coltivando inconsapevolmente un rapporto con un membro dei servizi segreti, o ancora involontariamente, se il giornalista o chiunque sia oggetto della ricerca, viene fatto sorvegliare o pedinare. Con una posizione di potere tale da essere secondi solo ai decisori, certo non desta preoccupazione il ricorrere ad attività illecite. Sia per i giornalisti sia per L'Intelligence, per lo meno quella parte inserita nel contesto mediatico al solo scopo di filtrare le informazioni , la verità non sembra ricoprire un ruolo di primaria importanza: I giornalisti cercano soprattutto il pezzo che fa notizia ingigantendo il più possibile anche ciò che sembra ovvio, L'Intelligence e quindi i decisori ripongono attenzione su cosa bisogna rendere pubblico e cosa va tenuto segreto. Per molte di queste informazioni viene utilizzato il principio di verosimiglianza allo scopo di attirare l'attenzione dell'opinione pubblica: la notizia che viene fornita, qualora non necessariamente vera o verificabile, deve sempre essere verosimile, cioè non lontana da quello che l'opinione pubblica si aspetti che accada. I Servizi di Intelligence ricorrono e metodi come la Disseminazione Coperta e L'Intossicazione Ambientale (Giannuli 2012). Nel primo caso, tramite la

triangolazione[7] vengono diffuse informazioni volutamente errate o modificate, da un soggetto che per "vendetta" o per coinvolgimento sembra voler passare queste informazioni direttamente dall'interno (ad esempio un dipendente del soggetto della notizia), nel secondo, invece, vengono inserite nell'ambiente mediatico numerose notizie apparentemente scoordinate ma destinate, tutte insieme, a spingere l'opinione pubblica sulla strada voluta. Il controllo mediatico sull'opinione pubblica quindi, scaturisce in parte dal controllo statale sui mezzi di comunicazione, creando una sorta di catena che le tecnologie più recenti stanno mettendo in discussione. Il Citizen Journalism, nel caso della rivolta Siriana ma in generale in tutto il contesto della Primavera Araba, ha messo in discussione il ruolo del medium giornalistico, non più cosi necessario, creando agitazioni nel mondo delL'Intelligence che trova difficoltà nel controllare le informazioni veicolate dai motori di ricerca o semplicemente dai cittadini stessi tramite i Social Network. Se appare chiaro che il fattore tempo sia la variabile più importante del giornalismo negli ultimi anni, allo stesso modo è possiamo comprendere il valore di una foto o di un video, prove registrate sul momento da cittadini come noi e non a posteriori da un giornalista straniero. Questo gap di controllo democraticizza l'informazione, del quale finora abbiamo sottolineato la negatività se coperta da un eccessiva manipolazione dei vertici, ma ne perde in qualità, ed è certamente facile cadere nella trappola di una foto *photoshoppata* o di un video ritoccato. Esemplare in questo contesto è l'esempio che fornisce Giannuli (2012): la storia di Amina, una blogger Siriana dichiaratasi omosessuale e per questo rapita a Damasco dall'esercito, si è rivelata una vera e propria bufala, inventata da una coppia scozzese per sensibilizzare l'opinione pubblica sulle condizioni di vita in Siria. Attirare l'attenzione dell'opinione pubblica risulta facile poiché molte di queste tecniche di manipolazione della realtà non sono conosciute o comunque perché tendiamo a fidarci dei mezzi di comunicazione, stesso non è per i decisori, in quanto fanno utilizzo delle stesse metodologie per gli stessi scopi. Ulteriori tecniche di manipolazione dell'informazione possono riguardare l'utilizzo di alcuni diversivi, come attribuire una verità troppo scomoda a una tattica dell'opposizione

[7] Attività che consiste nel coinvolgimento di un tramite apparentemente indipendente che diffonda la notizia.

politica, un smentita implicita, quando il soggetto che sembra essere stato "favorito" viene attaccato improvvisamente, l'utilizzo dei fattoidi, o di previsioni esageratamente ottimistiche per smontare la rilevanza di un risultato che, seppur ugualmente positivo, non eguaglia le previsioni stesse, o al contrario giustificare una serie di dati negativi inserendo statistiche ancora più scoraggianti appartenenti ad altre nazioni e cosi via. Ogni destinatario, poi, sarà percettore attivo, se si accorgerà delle incongruenze, passivo, se invece si farà influenzare totalmente, lettore privilegiato quando è a conoscenza delle dinamiche reali e del contesto, e diretto interessato, quando la notizia lo riguarda in prima persona. Certo è che ogni notizia, manipolata o meno, vera o verosimile, avrà più influenza quanto più è diversificato è il taglio, inserendola in più tipi di giornali, utilizzando più di una lingua e più di un mezzo di comunicazione.

Open Source Intelligence, la nuova sfida globale

E' necessario classificare i diversi tipi di raccolta delle informazioni all'interno dell'agenda dei Servizi Segreti per poter stabilire su quali di queste i nuovi media esercitano più influenza, su quali novità sono state introdotte nel mondo dello spionaggio negli ultimi decenni e quanto queste abbiano influito poi sull'effettivo andamento della politica internazionale. Abbiamo già parlato di OSINT, HUMINT e SIGINT, la collaborazione tra la racconta d'informazioni mediante fonti di pubblico accesso, contatti interpersonali e fonti umane, e quella mediante intercettazioni e analisi dei segnali ha cambiato il volto dello spionaggio. All'interno di queste possiamo selezionare ulteriori categorie, come l'IMINT (Imagery Intelligence), la COMINT (Communications Intelligence), la ELINT (Electronic Signals Intelligence), la TECHINT (Technical Intelligence) e la MASINT (Measurement and Signature Intelligence). L'OSINT, è certamente quella che più di tutti merita di essere osservata con una lente di ingrandimento. Il termine "fonti aperte" si riferisce a fonti liberamente accessibili, quindi certamente non coperte da segreto: mezzi di comunicazione, dati pubblici, fotografie, conferenze e lezioni e pubblicazioni. Una fonte aperta non è necessariamente gratuita, ad esempio può essere una pubblicazione molto costosa, e non è neppure sempre legale, come alcune tecnologie e mezzi di intercettazione disponibili solo ad esperti e specialisti del

settore. Per utilizzare al meglio queste fonti è necessario comprendere che esse sono ovunque, e che bisogna avere una visione più ampia poiché informazioni non di poco conto possono trovarsi anche all'interno di un necrologio. Inoltre, l'attività connessa all'Open Source non è solo "Intelligence che raccoglie informazioni *dalle* fonti aperte" ma anche "Intelligence comunica a*ttraverso* le fonti", quindi attività tanto attiva quanto passiva. La figura della spia, come abbiamo già detto, viene sostituita dalla figura dell'analista, che deve essere in grado di studiare ciò che si trova scritto ma anche ciò che si è cercato volutamente di evitare, e deve soprattutto essere in grado di consultare tutte le fonti e di non farsi confondere dalla sovrabbondanza di quest'ultime. L'OSINT, nonostante ancora non venisse identificata con questo acronimo, fa parte dello spionaggio tradizionale già dai primi del Novecento (ad esempio ne fece uso l'OVRA fascista) ma come è facile immaginare, è sempre stata un'attività considerata di scarso valore, in primis perché nelle fonti di pubblico accesso non sono mai presenti dati politici o militari rilevanti, perché sempre coperti da segreto di stato, in secondo luogo perché appariva inutile utilizzare dei dati che potevano essere disponibili anche per i nemici, e poi perché in tempo di guerra, articoli e bollettini fornivano previsioni esageratamente ottimistiche e di conseguenza poco attendibili. Solo nei primi anni '50 con la Guerra Fredda, l'utilizzo delle fonti aperte si è reso, più che utile, necessario. Spie americane e tedesche tentarono di studiare la società russa ma la maggior parte di questi venne catturata e uccisa dall'apparato militare russo, di conseguenza per evitare ulteriori morti si iniziò a reperire informazioni direttamente dalla stampa nazionale, scomponendo e interpretando le notizie. Negli anni 90' l'OSINT accrebbe il proprio successo grazie alla globalizzazione economica e all'integrazione politica ma anche grazie alla marginalizzazione dell'origine militare dello spionaggio. Internet, come mezzo di comunicazione che viene messo a disposizione di tutta la popolazione occidentale, permettendo l'accesso a un infinito numero di database contenenti un altrettanto infinita quantità di dati rilevanti, ha permesso all'Open Source Intelligence di acquisire in quegli anni sempre più rilevanza. Convenienza, soprattutto, in quanto l'OSINT richiede una quantità di risorse economiche decisamente più bassa del HUMINT e del SIGINT; in più le risorse non essendo coperte da segreto sono facilmente

reperibili e quindi la raccolta risulta particolarmente fiorente anche in un lasso di tempo brevissimo. Chiaramente la velocità e la semplicità con cui le informazione possono essere radunate viene compensata dai lavori di classificazione e di analisi, che come abbiamo già detto richiedono una particolare tipologia di analisti mediatici, ma nonostante ciò appare difficile negare l'utilità e la flessibilità dell'Open Source Intelligence, elemento ormai irrinunciabile per qualsiasi apparato statale di raccolta delle informazioni.

Cyber Intelligence: il world wide web al servizio dei decisori

Che le nuove tecnologie, con la loro pervasività, abbiano sconvolto ogni processo decisionale, politico o economico che sia, sembra una banalità. Ma anche la guerra vera e propria ha subito dei mutamenti, e cosi accanto ai conflitti armati che da secoli dominano la società, si sta affiancando una nuova minaccia che può, al pari di una guerra combattuta con le armi da fuoco, mettere in crisi la società e distruggerne le fondamenta. La Cyberwar o *Cyberwarfare* è l'insieme delle attività informatiche funzionali alla distruzione dell'informazione avversaria. Le metodologie dei cyber attacchi vanno dal semplice vandalismo web, alla raccolta di dati altrimenti segreti, la distruzione delle apparecchiature, dei server o dei software e per ultimo anche dei servizi di prima necessità forniti dalle nazioni attraverso le tecnologie più avanzate. Questo tipo di attacco viene sempre di più avallato dalle organizzazioni o dai partiti antisistema poiché, in primis, esiste ancora poca giurisdizione in materia, in secondo luogo la pianificazione e l'esecuzione degli attacchi è decisamente più economica di qualsiasi altro tipo di conflitto armato, perché gli attacchi sono tempestivi e immediati; infine, dato non da sottovalutare, il Cyberterrorismo permette all'attentatore di restare completamente anonimo. Questa minaccia può concretizzarsi anche attraverso i Social Network tramite il *Social Poisoning,* attività che consiste nella vera e propria sostituzione identitaria per ottenere informazioni, ma anche attraverso *botnet* una rete di PC infettati da virus che, collegandosi, possono collegarsi e infettarne altri. Il numero di hacker e cracker è in continua crescita, ed è singolare come, nonostante le due attività siano illecite, governi e servizi di Intelligence arrivino a farne uso per difendere i propri sistemi informatici. L'obiettivo centrale del cyber

spionaggio è quello di reperire informazioni segrete facendo uso delle più elevate tecnologie, il che richiede sia un coinvolgimento delle risorse umane che delle risorse informatiche. Negli Stati Uniti sono stati riscontrati diversi attacchi, nello specifico le responsabilità dei due esempi più famosi, passati alla storia come *Titan Rain* e *Moonlight Maze* sono state attribuite ad hacker russi e cinesi. Nel primo caso si trattò di una serie di attacchi a "pioggia" contro computer di tutta l'America, il che permise agli autori, probabilmente appartenenti al corpo militare cinese, di accedere a molte reti informatiche tra cui quella della NASA; nel secondo caso similmente i sistemi *hackerati* furono quelli del Dipartimento di Difesa, questa volta però la responsabilità venne attribuita ai Russi in quanto il computer da cui proveniva l'attacco era stato localizzato a Mosca. Sempre in Russia, l'azienda Kaspersky, specializzata in prodotti per la sicurezza informatica, ha individuato diverse campagne di Cyberspionaggio, come *Flame, Gauss, Net Traveler* e *Icefog.* In particolare nell'atto di studiare i primi due, i maggiori esperti informatici dell'azienda hanno riscontrato come l'obiettivo dei Trojan[8] non fosse tanto dettato da interessi di tipo economico, ma anzi sembrava che chi l'aveva progettato volesse colpire proprio le infrastrutture nazionali. Meno di un anno fa, lo stesso laboratorio di analisi della Kaspersky, ha scoperto un'altra operazione di Cyber Spionaggio, il malware estremamente evoluto a cui hanno dato nome *Red October,* il quale ha colpito, in soli cinque anni, ambasciate e governi evolvendosi e diffondendosi tramite Microsoft Office ed Excel. Sempre nel 2013 sono stati individuati anche altre campagne di Cyberspionaggio: l'operazione *Winnti*, attribuita ad un gruppo di cyberterroristi cinesi, ha attaccato numerose aziende di videogiochi per trafugare codici di videogiochi in progettazione, i programmi malware chiamati *Net Traveler* hanno colpito maggiormente il settore energetico, quello nucleare, l'industria farmaceutica, la tecnologica e l'industria delle comunicazioni; infine nell'operazione *Icefog,* che ha interessato obiettivi localizzati in Corea del Sud e in Giappone, ha portato alla luce una nuova categoria di Hacker, quella dei "mercenari" cibernetici (Wikipedia) che attaccano in gruppo settori ancora più delicati, come il marittimo e il militare. In questo caso vengono utilizzati Virus,

[8] Software progettato per danneggiare il sistema informatico in cui viene eseguito

Warm o Trojan e poi tramite la tecnica dello *Spear Phishing*[9] l'autore dell'attacco collega il proprio computer con quello della vittima, infettandolo. Il Cyberterrorismo può portare alla sottrazione di informazioni dal valore incalcolabile, di nuovo L'Intelligence si trova a dover affrontare una minaccia nuova, forte, giovane e difficilmente affondabile. Come affrontare la *Cyberwarfare*, dunque? abbandonando le tecnologie, come nel caso Russo, dove secondo il quotidiano Izvestia, il Federal Protective Service sta lentamente sostituendo parte dei computer con delle vecchie ma costose macchine da scrivere? Sarebbe certamente più produttivo mettere da parte la vecchia Intelligence Informativa e affidare la sicurezza delle nazioni ai più esperti informatici del mondo.

[9] Tramite una email che sembra provenire da qualche conoscente, con lo Spear Phishing un Hacker riesce ad entrare nel sistema informatico di colui che apre l'email, può quindi perpetrare una frode, rubare password e codici, o anche infettare il PC con un Virus .

Capitolo quarto – Case Studies, confronto tra Italia, Unione Europea e Comunità Internazionale

Fallimento delL'Intelligence nel Decennio Breve: 9/11, Madrid, Londra

Catapultando le teorie della rivoluzione digitale e della nuova Intelligence comunicativa sugli eventi più significativi degli ultimi quindici anni di storia del terrorismo, non possiamo non notare che i più catastrofici attentati della storia si sono verificati proprio in Occidente, nel momento che forse meglio poteva fornire la possibilità di prevedere e le armi per prevenire. L'attentato alle Torri Gemelle è considerato forse il primo grande fallimento della CIA, cosi come i vicinissimi attentati di Londra e di Madrid. La tesi più gettonata è che la modernizzazione abbia cambiato il mondo cosi in fretta che la rivoluzione digitale abbia creato delle crepe, delle crisi sistemiche in occidente, e che alcuni tipi di minacce non siano ancora pronte per essere combattute. Il terrorismo è certo un tabù della società globalizzata, poiché da un lato si cerca di sviluppare continua interdipendenza politica, sociale ed economica attraverso la Globalizzazione, ma dall'altro ancora le nazioni non hanno stabilito nemmeno una definizione comune della parola "terrorismo": risulta quasi una banalità che la più pericolosa forma di criminalità debba essere combattuta singolarmente dagli stati, e solo da quelli che la riconoscono come minaccia alla sicurezza nazionale. La dipendenza occidentale dal petrolio, certo, non facilità la conduzione della "guerra al terrorismo", cosi come l'attenzione verso pericoli più imminenti, come l'economia sommersa, i traffici illeciti, la sicurezza industriale e aziendale. Ridefinire i "consumatori di Intelligence" (Steele, 2002) dovrebbe essere una delle priorità delle potenze occidentali, non solo perché gli insuccessi dei Servizi di Informazione sembrano nascere dall'idea che questi siano pagati per difendere gli apparati burocratici, più che la nazione che rappresentano, ma anche perché un popolo digitalizzato non vuole, anzi, non può essere tenuto all'oscuro di una sostanziosa parte dell'informazione. Anzi la repressione, in questo senso, può portare allo scavalcamento delle Istituzioni di chi, tramite l'abilità informatica, riesce a disporre come meglio crede di una conoscenza da cui sarebbe legalmente escluso. Il settore comunicativo e i digital media, collaborando con gli 007 del ventesimo

secolo, potrebbero istruire una generazione informata e recettiva, aumentare la competitività e stabilire una nuova frontiera per gli investimenti, e questo solo mostrando come la nazione possa gestire il proprio apparato informativo coinvolgendo tutta la collettività, non solo una parte. "Citizen Intelligence" (Steele, 2002) in cui "ciascun cittadino deve essere un raccoglitore, produttore e utente di *Intelligence*" è un concetto che vuole rivendicare il diritto dei cittadini a relazionarsi con tutti i fenomeni politici ed economici che sono all'ordine del giorno potendo ricorrere alle stesse fonti aperte a cui ricorrono i Decision Makers. Troppa segretezza equivale a troppo costo, ad un tipo di spionaggio non più attualizzabile, ridicolo se vogliamo, considerando la facilità con cui le notizie oggi possono essere reperite. Per quanto riguarda le varie Organizzazioni Internazionali che tendono a regolare i rapporti tra le nazioni, la sicurezza viene di certo messa in primo piano dalla NATO, l'articolo quinto del Patto Atlantico chiarisce che "un attacco armato contro una o più di esse, in Europa o in America settentrionale, deve essere considerato come un attacco contro tutte" e che ovviamente ogni nazione è tenuta a prendere "immediatamente, individualmente o in concerto con le altre parti, tutte le azioni che ritiene necessarie, incluso l'uso della forza armata, per ripristinare e mantenere la sicurezza dell'area Nord Atlantica". Anche l'Unione Europea ha approvato nel 2010 la "Strategia di Sicurezza Interna per L'Unione Europea", il quale risulta essere il primo vero e proprio documento che tenta di formulare un modello a difesa della sicurezza dell'Unione. Tra le minacce principali appare il Terrorismo, che anzi è inserita graficamente al primo posto, il riciclaggio, il crimine organizzato, la corruzione e la Cyberwar. Il rapporto tra l'Organizzazione del Nord Atlantico e l'Unione Europea nell'ambito della difesa e della sicurezza non è ancora chiaro, ad esempio fanno entrambe riferimento alla tutela dei diritti umani e in generale alla difesa della pace, però dall'altro lato l'Unione ha condannato le *Extraordinary Renditions*[10], poiché misero in discussione alcuni dei principi fondanti dell'Unione stessa. Quest'ultima, con i suoi ventotto stati membri, non deve soltanto rispondere alle nuove minacce globali, al terrorismo internazionale e alla crisi economica, ma deve

[10] Operazione extralegale di cattura e detenzione eseguita nei confronti di un soggetto accusato di terrorismo. Un esempio è il caso di Abu Omar in Italia.

sopra ogni cosa mettere in relazione gli interessi di tutti gli Stati membri, i quali manifestano priorità diverse, egoismi nazionali, interessi e alleanze contrastanti, soprattutto in materia di difesa. Di conseguenza anche la politica di sicurezza sarà indirizzata alla protezione degli Stati membri, più che alla lotta al terrorismo islamico, anche se viene comunque considerato un obiettivo all'interno della Strategia di Sicurezza Interna. Mai come in quest'anno, che è stato caratterizzato dalle Elezioni Europee, si sono manifestate minacce all'UE più incombenti del Terrorismo. Nazionalismi, numerosi seggi ai partiti euroscettici, forti populismi e movimenti estremisti. Per quanto riguarda il cyberterrorismo, d'altro canto, due eventi in particolare hanno catapultato nella rappresentanza dell'Unione, la consapevolezza dei nuovi pericoli della società digitalizzata. In Estonia nel 2007 e in Georgia nel 2008[11] (la quale, seppur non membro dell'UE, ha firmato accordi per il libero scambio e di associazione), sono stati perpetrati due dei cyberattacchi più famosi della storia, i quali hanno suscitato allarmismi in seno all'Unione, in primis circa l'importanza di innalzare una barriera di difesa in campo informatico, e anche riguardo la necessità di integrazione all'interno dell'organizzazione, se non militare, quantomeno tra i Servizi Segreti. Sembra che quest'anno l'UE abbia preso in seria considerazione questo tipo di minaccia, poiché l'alto rappresentante Catherine Ashton insieme alla Commissione Europea hanno elaborato il primo documento strategico dell'Unione per la Sicurezza Informatica[12]. Sul modello Estone[13], il Regno Unito ha creato una struttura per la cyberdifesa, il *Fusion Cell.* Programmata per essere un circuito collaborativo finalizzato alla lotta contro il cyberterrorismo e lo spionaggio informatico, questa sviluppa la propria politica sulla base dell'idea che la tutela dei sistemi informatici aziendali e industriali sia indispensabile al salvaguardia della sicurezza dell'intera nazione. Questi ultimi esempi dimostrano come ci si stia rendendo conto che L'Intelligence debba basarsi su obiettivi generici di interesse nazionale, la difesa al primo posto, anche se in alcuni paesi è l'interesse della maggioranza a prevalere. L'Intelligence Italiana, a fronte dell'enorme capacità organizzativa, non riesce ad individuare gli obiettivi su

[11] Due tentativi di oscurare il sistema Informatico in cui vennero paralizzate le banche, gli uffici governativi e i media network; in entrambi i casi si attribuisce la colpa ad Hacker Russi.
[12] Cyber Security Strategy of the European Union
[13] In Estonia è stato collocato il Cooperative Cyber Defence Center of Excellence della NATO

cui dovrebbe fondarsi il carico di lavoro: spesso gli scontri ideologici interni, e quindi le esigenze della maggioranza o della classe politica in generale, oscurano la politica estera che quindi viene lasciata da parte. La carenza di punti di vista tutti Italiani sulla scena internazionale e la scarsità di emancipazione culturale dovuta a decenni di influenza statunitense, rendono ancora più difficile il predisporre L'Intelligence a combattere le digitali quanto planetarie minacce globali.

WikiLeaks, il Quinto Potere contro il Segreto di Stato

Il più famoso esempio del collasso tra segreto di stato e digital media è certamente il caso Wikileaks. Creata dall'australiano Julian Assange, questa organizzazione internazionale senza scopo di lucro ha come scopo quello di pubblicare documenti (ricevuti ovviamente in modo anonimo) coperti da segreto di Stato sul proprio sito web. Cittadini da ogni parte del mondo possono inviare materiale sensibile, e il sito stesso, con un sistema di cifratura, riesce far si che questi rimangano totalmente anonimi. Ovviamente la pubblicazione di materiale coperto da segreto è assolutamente illegale, ma gli attivisti di Wikileaks vogliono affermarsi come promulgatori di una maggiore trasparenza, di conoscenza garantita a tutti e di una maggiore democrazia. Il sito, lanciato nel 2006, pubblicò in pochissimi anni un numero quasi illimitato di intercettazioni telefoniche, a cominciare da quelle di alcuni hacker cinesi nell'atto di cercare informazioni sui governi occidentali (Wikipedia), informazioni sull'equipaggiamento militare americano durante la guerra in Afghanistan, numerosi dispacci contenenti prove inconfutabili della corruzione in alcuni paesi dell'Africa e documenti che attestavano violazioni dei diritti umani nelle prigioni di Guantánamo. Ciò che fece più scalpore furono i documenti riservati dell'esercito statunitense e iracheno in cui erano descritti gli abusi e le torture perpetrate durante la guerra in Iraq. Il caso Wikileaks rappresenta uno degli snodi cruciali della rivoluzione informatica. E' la testimonianza del fatto che L'Intelligence necessita dei cambiamenti, poiché rischia di essere superata in scaltrezza da un gruppo di civili, esperti informatici, certo, ma pur sempre privi di un vero e proprio addestramento militare. Un ulteriore fallimento dei servizi di sicurezza ed informazione, dunque, che porta alla luce le evidenti carenze delle strategia contro il cyberterrorismo, una minaccia che si

propone più attuale e potenzialmente più distruttiva di una guerra combattuta con le armi da fuoco. Non esistono prove, tuttavia, che la redazione freelance di Assange non sia in realtà manipolata da un servizio di Intelligence al fine di scatenare un gigantesco conflitto informatico. Oppure, che vi siano dietro interessi puramente economici, considerando l'attacco a banche come la svizzera Julius Baer e la pubblicazione di una lista contenente più di due mila proprietari di conti offshore. Julian Assange è una figura emblematica di questo decennio, da un lato accusato di spionaggio e tradimento, additato come criminale e alla continua ricerca di un'ambasciata in cui rifugiarsi, dall'altro lato, candidato al premio Nobel per la Pace per il suo contributo alla lotta per la libertà d'informazione. Il conflitto che la quantità di dati in circolazione attraverso Internet e tutta la rivoluzione digitale stanno portando alla luce, inizia a mettere in crisi le relazioni internazionali, al punto che un hacker attivista come Assange e tutti i suoi collaboratori si ritrovano ad essere considerati allo stesso tempo eroi e criminali, difensori di un diritto inalienabile quale la libertà d'informazione, ma allo stesso tempo perseguitati da una continua caccia all'uomo, sotto innumerevoli capi d'accusa. Il conflitto tra segreto di stato e trasparenza globale, non sembra ancora aver messo d'accordo le grandi potenze democratiche.

Datagate: Privacy, riservatezza, sicurezza.

Le democrazie occidentali basano la loro legittimazione sulla difesa dei diritti dei cittadini che le hanno legittimate come sovrane. Ora, quando la difesa di due diritti fondamentali come il diritto alla sicurezza e il diritto alla privacy vengono a scontrarsi, è difficile stabilire una politica comune. Ad esempio, la Dichiarazione Universale dei Diritti Dell'uomo, l'articolo 3 recita "Ogni individuo ha diritto alla vita, alla libertà ed alla *sicurezza* della propria persona", ma è certo che la sicurezza di una nazione debba essere garantita attraverso pratiche spesso extralegali. L'articolo 12, pur non parlando di privacy, afferma "Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione", ma ci si chiede se, nel caso in cui queste *interferenze* possano in qualche modo garantire la sicurezza di qualcuno, se il diritto possa essere

scavalcato. Il cosiddetto scandalo *Datagate* ha portato alla luce una verità che divide l'opinione pubblica, tra lo scandalo e l'ovvietà, tra l'indignazione per la mancata fiducia nelle relazioni internazionali, e la consapevolezza che qualsiasi nazione è spinta ad attivare la propria Intelligence non esclusivamente contro le organizzazioni terroristiche. Nel 2012 l'ex tecnico della CIA e consulente della NSA Edward Snowden, rivelò l'esistenza di software di spionaggio informatico, come *Xkeyscore* e il programma *Tempora,* e in generale di un sistema di intercettazioni che stava colpendo tutta l'Europa, dai civili ai trentasei capi di stato. Due giornalisti di *The Guardian* (Glenn Greenwald e Laura Poitras) vennero forniti di più di ventimila documenti Top Secret da cui attingere per verificare le scottanti rivelazioni. Uno scandalo, certo, ma non completamente. All'interno della categoria di SIGINT, L'Intelligence che si occupa dei segnali elettromagnetici, viene collocata la categoria di COMINT (Communications Intelligence), la quale raccoglie le informazioni derivanti dalla comunicazione tra due soggetti. Perché stupirsi, allora, quando Snowden rivelò il programma di intercettazioni di massa della National Security Agency? Perché colossi del web a cui ci affidiamo quotidianamente, come Facebook, Google, Apple e Yahoo hanno garantito alla NSA libero accesso alle informazioni degli utenti? Perché gli Stati Uniti hanno intercettato le comunicazioni delle sedi diplomatiche e dei leader europei? Bisogna considerare che gli Stati Uniti rispondono al Patriot Act[14] e al Foreign Intelligence Surveillance Act[15], e che in generale la difesa della sicurezza nazionale prevale come diritto sopra a tanti altri. Anziché abbandonarsi all'utopia di una macroalleanza globale, in cui tutte le nazioni dovrebbero fidarsi delle altre, bisognerebbe partire dal presupposto che ogni nazione vuole perseguire il proprio interesse, e che dunque non si dovrebbe cedere all'isteria di fronte ad uno "scandalo" che poi, per quanti precedenti ha avuto, scandalo non sembra. Il caso Echelon ne è un esempio: scoppiato nel 1998, ha rivelato l'esistenza di un sistema

[14] "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" è una legge federale che rafforza i poteri dei corpi di polizia e spionaggio statunitensi, quali CIA, FBI e NSA con lo scopo di ridurre il rischio di attentati terroristici negli Stati Uniti (Wikipedia)

[15] Atto normativo statunitense che detta le procedure di sorveglianza fisica ed elettronica e per la raccolta di informazioni per L'Intelligence straniera messe in atto da potenze straniere negli USA (Wikipedia)

di reti di spionaggio costituite durante la Guerra Fredda dai servizi segreti americani, inglesi, neozelandesi, australiani e canadesi (AUSCANNZUKUS). Con il passare degli anni l'obiettivo della rete informativa si spostò dalla Russia sovietica a semplici attività governative, industrie ed imprese di tutto il mondo; il sistema venne poi portato alla luce dal rapporto STOA del parlamento Europeo. Come non citare, infine, come ulteriore esempio di scandalo dovuto ad intercettazioni di questo tipo, il caso Watergate, che negli anni settanta costò la presidenza a Richard Nixon. Costi irrisori e potentissime tecnologie permettono ai servizi segreti di ottenere informazioni di ogni tipo su qualsiasi soggetto gli interessi, e già negli anni settanta, dove il tutto appariva più difficile e si necessitava un maggior coinvolgimento dello HUMINT, non si riscontrò tutta questa sorpresa. Forse in piena Guerra Fredda, con la paura di una guerra nucleare dietro l'angolo, nessuno se la sentì di lamentarsi dello spionaggio, nonostante già tutti sapessero che gli Stati Uniti e l'Unione Sovietica stessero finanziando non poco L'Intelligence. Oggi i mezzi sono a disposizione di tutti, e anche se la Privacy viene tutelata dalle nazioni singolarmente, è chiaro come tutte queste regole non possano valere per i servizi di sicurezza. Riprendendo il tema del lettore mediatico attivo e passivo, questo potrebbe essere un esempio più che calzante. Un attore passivo, da questa storia, respirerà aria di scandalo: "Gli americani ci stanno spiando", e niente di più complesso che semplice indignazione. Un lettore attivo, qualcuno che ha compreso la relazione tra Intelligence e Media, non vedrà nulla di nuovo, ma ne dedurrà alcune informazioni interessanti. Innanzitutto il deterioramento del rapporto tra Stati Uniti e la due nazioni che hanno offerto asilo al "traditore" Snowden, Cina e Russia. Poi, la probabile riduzione dei finanziamenti alla CIA e alla NSA, Intelligence rea di aver fallito più di una volta negli ultimi quindici anni, dall'attentato alle Twin Towers, alla maratona di Boston, passando per il caso di Julian Assange e del fenomeno di Wikileaks. Concludendo, il caso Snowden, presentato dall'industria mediatica come un simbolo del controllo statunitense sull'Unione, andrebbe osservato con una diversa chiave di lettura, più personale, staccata dai telegiornali o almeno ragionata. L'Intelligence nasce dallo spionaggio, come le si può chiedere di non fare ciò per cui è nata?

Conclusione: Sfide del mondo contemporaneo

*Adattare L'Intelligence alla digital era, senza distaccarla dagli interessi dei cittadini, e da essa imparare a 'servirsi dei nuovi media senza servirli' (*Balassone, 21, sd)

Che L'Intelligence abbia un ruolo significativo nella politica militare nazionale, ormai lo diamo per scontato. L'importanza dei Servizi di Informazione era stata già compresa dalle prime grandi civiltà, e non solo da quelle occidentali. Certo è che con l'avanzare delle tecnologie, delle cosiddette "guerre moderne" del ventesimo secolo, e del coinvolgimento sempre più forte dei civili, è cresciuta parallelamente anche la consapevolezza del ruolo dei Servizi Segreti. L'attività di spionaggio coinvolge soprattutto gli stati democratici, e non necessariamente in tempo di guerra, ma costantemente e non solo legato alla sfera militare. Vivendo in questa realtà, una realtà in cui le alleanze e i trattati internazionali forgiano delle relazioni, non possiamo negare che l'altra faccia della medaglia internazionale riveli che gli interessi nazionali sono stati e sempre saranno l'obiettivo primario di ogni stato. Appurate queste affermazioni, la Globalizzazione e la rete Internet fornendo la possibilità, sia culturalmente che digitalmente, ad ogni soggetto di connettersi con chiunque altro, ad un prezzo bassissimo, praticamente ovunque e con una velocità sempre più straordinaria, permettono ai servizi di informazione di reperire con estrema facilità informazioni su chiunque si sia mai connesso. Adattare L'Intelligence all'era digitale significa creare una rete globale di servizi segreti che rispondano alle nuove minacce, come Cyber Warfare e Terrorismo, di cui si è ampiamente discusso, attraverso l'Information Peacekeeping, sfruttando, quindi, le informazioni e l'informatica "allo scopo di conseguire obiettivi politici nazionali senza impiegare la violenza" (Steele, 257, 2002). Se i media hanno creato un sostituto virtuale dell'identità tramite i Social Network o i videogiochi MMORPG[16], cosi L'Intelligence deve utilizzare questi strumenti, non più, come ha fatto finora, per diffondere o nascondere le informazioni al pubblico di massa (attività che ad oggi ha solo portato a fenomeni di ribellione e di hacking di cui Wikileaks e

[16] è un gioco di ruolo per computer o console che viene svolto tramite Internet contemporaneamente da più persone reali, per questo si chiamano giochi "online". Migliaia di giocatori possono interagire interpretando personaggi che si evolvono insieme al mondo persistente che li circonda ed in cui vivono (Wikipedia)

Datagate sono due lampanti esempi) ma per convertire la guerra armata in una nuova forma di conflitto non violento, *cybercombattuto.* Cosi, dal modo in cui viene addestrata L'Intelligence, all'intera concezione dei conflitti, ogni elemento necessita una conversione per affrontare le nuove sfide globali. Per quanto riguarda i civili, per avere un chiave di lettura dei cambiamenti che la società globale sta affrontando, dalla *primavera araba* fino ai più recenti conflitti occidentali, l'utilizzo passivo dei media deve lasciare spazio ad una conoscenza pubblica, ad una trasparenza globale. Gli studi di Intelligence dovrebbero essere resi pubblici: un più alto livello d'istruzione della popolazione potrebbe, forse, mettere in difficoltà le classi dirigenti, ma non gli interessi della nazione i quali, supponendo che si realizzi questa eventualità, potrebbero essere innanzitutto compresi dai cittadini, e poi perseguiti da tutti. Il "cliente" delL'Intelligence non dovrebbe essere il governo né il vertice di un'azienda, ma la collettività. D'altra parte la manipolazione delle informazioni è una pratica che diventa ogni giorno più obsoleta in quanto le fonti aperte sono una realtà accessibile a chiunque, la novità sta nel fatto che oggi L'Intelligence può avere un ruolo significativo nella tutela della cultura e della sicurezza nazionale, non per ciò che compie da sola e per conto dei decisori, ma per la possibilità di evolversi tramite la connessione con le altre agenzie di Intelligence sparse in tutto il mondo, e per il potere che può fornire alla cittadinanza tramite la *distribuzione della conoscenza.* Condividere l'informazione, utilizzarla per difendere gli interessi nazionali e la sicurezza del proprio paese, sfruttare la capacità aggregativa dei media network per evolvere e non per controllare, mantenere saldo l'equilibrio tra privacy e conoscenza necessaria, così come tra il segreto di stato e la trasparenza che si richiede ad una società globalizzata. queste sono le sfide a cui L'Intelligence sarà chiamata a rispondere nei prossimi decenni.

Bibliografia

Testi

Balassone, S. (SD) *I Mass Media fra società, potere e mercato.(Book-In-Progress)*

Ceci, A. (2007) *Intelligence e Democrazia, la relazione responsiva nella società della comunicazione.* Soveria Mannelli (Catanzaro): Rubbettino.

Colonna Vilasi, A. (2011) *Manuale d'Intelligence.* Reggio Calabria: Città del sole edizioni s.a.s.

Giannuli, A. (2012) *Come i servizi segreti usano i media.* Pioltello (Milano): Adriano Salani Editore S.p.A.

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

Articoli Online

Carracciolo, L. (2013) Geopolitica per l'Intelligence. *Gnosis* [Online] (3/2013) p 59-65. Disponibile in *http://gnosis.aisi.gov.it/gnosis/Rivista36.nsf/ServNavig/36-20.pdf/$File/36-20.pdf?OpenElement* [Accesso 07/2014]

Luttwak, E., Gaiani, C. (2013) Intelligence e Intercettazioni . *Gnosis* [Online] (4/2013) p 117-127. Disponibile in *http://gnosis.aisi.gov.it/Gnosis/Rivista37.nsf/ServNavig/37-21.pdf/$File/37-21.pdf?openElement* [Accesso 07/2014]

Magri, P., Venturini, F., Del Re E.C. (eds), (2013) Sicurezza Europea, le nuove sfide. *Gnosis Forum*[Online] (1/2013) p 3-22. Disponibile in *http://gnosis.aisi.gov.it/gnosis/Rivista34.nsf/ServNavig/34-57.pdf/$File/34-57.pdf?OpenElement* [Accesso 07/2014]

Teti, A. (2013) 'Fusion Cell' una struttura per la Cyberdefence. *Gnosis* [Online] (2/2013) p 75-83. Disponibile in *http://gnosis.aisi.gov.it/Gnosis/Rivista35.nsf/ServNavig/35-11.pdf/$File/35-11.pdf?OpenElement* [Accesso 07/2014]

Teti, A. (2013) Cyber Intelligence e Cyber Espionage: come cambiano i servizi di Intelligence nell'era del Cyberspazio. *Gnosis* [Online] (3/2013) p 95-121. Disponibile in *http://gnosis.aisi.gov.it/Gnosis/Rivista36.nsf/ServNavig/36-21.pdf/$File/36-21.pdf?openElement* [Accesso 07/2014]

Websites: Wikipedia [Accesso, 07/2014 – 10/2013]