Cyber Warfare 2014

Armi cibernetiche, sicurezza nazionale e difesa del business

a cura di Umberto Gori
e Serena Lisi

CWC 2015 CYBER WARFARE CONFERENCE

FrancoAngeli

Cultural e Cyber Intelligence: la Nuova Alleanza?

di *Alessandro Zanasi*[1]

1. Introduzione

Ottant'anni orsono un importante politico tedesco asseriva di portare istintivamente la mano alla pistola ogni qualvolta sentiva pronunciare la parola "cultura".

Sessant'anni fa, in risposta ad un interlocutore che sottolineava la potenza del Papa, un politico russo chiedeva di quante divisioni disponesse quest'ultimo (lasciando intendere che per lui il potere intangibile non esistesse).

Pochi anni orsono un politico italiano osservava sarcasticamente che la cultura non si mangia.

Tutti e tre questi uomini politici diedero prova di poca sensibilità a fattori intangibili come quelli culturali. Il fatto che tutti e tre siano poi stati sconfitti dalla storia ci spinge giocoforza a riflettere sull'importanza, spesso colpevolmente trascurata, che i fenomeni culturali rivestono nelle nostre società.

---

[1] Fondatore e CEO di *Zanasi & Partners* (Z&P), società specializzata in sicurezza ed intelligence, formata da ricercatori e consulenti con competenze ed esperienze acquisite lavorando presso la Commissione Europea (ESRAB ed ESRIF), in società informatiche (IBM) e nucleari (Ansaldo), in centri di ricerca (in Francia, Stati Uniti e Italia), nelle forze dell'ordine (Carabinieri) e svolgendo attività accademiche (in Francia, Regno Unito ed Italia). Sito web: http://www.zanasi-alessandro.eu

Si ringrazia il dott. Alessandro Bonzio, ricercatore di Z&P, per l'importante contributo fornito nella preparazione di questo scritto.

In un contesto di forte interconnessione e multietnicità come quello dell'attuale scenario globale, infatti, la comprensione della cultura altrui rappresenta un fattore cruciale per intuire motivazioni, interpretare comportamenti e, in alcuni casi, arrivare a prevedere le azioni di soggetti che provengono da contesti completamente diversi dai nostri. Se per il comune cittadino tale conoscenza è alla base della capacità di relazionarsi in modo costruttivo con il "diverso", essa diventa addirittura indispensabile quando occorre fronteggiare attori potenzialmente ostili. In ambito militare, la conoscenza della cultura del nemico può risultare cruciale per il successo di una missione, in particolar modo se condotta in terra straniera. Le recenti campagne in Afghanistan ed Iraq hanno dimostrato quanto elevati possano arrivare ad essere i costi di una conoscenza limitata della cultura locale per tutte le forze in gioco. Se si considera poi che una delle principali minacce alla sicurezza fronteggiate oggi dall'Occidente è di matrice non più statale bensì ideologica – ispirata ad interpretazioni fondamentaliste della religione - appare ancor più evidente l'importanza di comprendere a fondo l'insieme di valori, credenze e attitudini alla base dell'operato di chi orbita nella galassia dell'estremismo.

E' in questo quadro che va ad inserirsi il concetto di *cultural intelligence* inteso come l'attività di intelligence condotta sulla base di informazioni di carattere sociale, politico, economico e demografico in grado di favorire la comprensione della storia, delle istituzioni, della psicologia, delle credenze e dei comportamenti di una nazione o di una popolazione[2]. Con questo termine non ci riferiamo ad una nuova forma di intelligence ma ad una particolare branca di essa che, seppur pesantemente sottovalutata nel corso degli ultimi decenni, promette di avere un impatto sempre più significativo in ambito di sicurezza. E' ormai chiaro che superiorità tecnologica e militare non siano sufficienti a sconfiggere entità che - come al Qaeda o il sedicente Stato Islamico (IS) – si affidano a strategie di guerra asimmetrica e non convenzionale. Inoltre, come sottolineato da McFate, il principale nemico che le potenze occidentali dovranno affrontare in futuro sarà «non occidentale nell'orientamento, transnazionale nello scopo, non gerarchico nella struttura e clandestino nei propri approcci»; una forza che opererà al di fuori del sistema degli stati nazionali e le cui motivazioni, strutture e metodi di combattimento saranno in larga misura determinati dalle rispettive società e culture di provenienza[3].

[2] Coles (2005).
[3] McFate (2005), citato in Vivaldi (2014).

Scrivere di cultural intelligence appare oggi necessario anche se rischioso ed audace. In special modo se cerchiamo di affrontare il tema facendo riferimento allo scenario della cyberwarfare. Il provocatorio titolo di questo articolo, che si rifà al famoso saggio del premio Nobel Ilya Prigogine e di Isabelle Stengers[4], lascia intendere quale ne sia l'ambizione. Cultura umanistica e cultura tecnica non sono assolutamente da intendersi in contrasto tra loro, anzi. E ciò è ancor più vero nella disciplina che più, dal 2001 in poi, è stata oggetto di attenzione e revisione, ovvero l'intelligence, alla ricerca di spiegazioni, anche cognitive, dei suoi "fallimenti".

Il presente articolo si pone l'obiettivo di illustrare il ruolo che la cultural intelligence è destinata a ricoprire nel nuovo millennio, evidenziandone lo stretto legame con i più recenti sviluppi nel campo della tecnologia, in particolare con quello che riguarda Internet e la derivante capacità di condividere l'informazione, recuperarla (*information retrieval*) ed analizzarla automaticamente (*big data analytics, data e text mining*). In una parola: *cyber intelligence*. La diffusione pervasiva di Internet e dei *social media* (es. Twitter, Facebook, YouTube) ha infatti reso possibile la raccolta di cultural intelligence in misura impensabile prima d'ora. Il Web si è rapidamente imposto come mezzo di comunicazione imprescindibile non solo per molti comuni cittadini ma anche, come spesso accade con le nuove tecnologie, per gruppi criminali e terroristici di varia natura.

Dopo una presentazione della cultural intelligence e dei fattori che spingono oggi verso una sua riscoperta (specialmente alla luce del grave attentato dello scorso 7 gennaio a Parigi, il quale può essere interpretato come un "attacco culturale", con la conseguente necessità, per comprenderlo, di introdurre categorie quali laicità e laicismo, islamismo ed ebraismo, scontri tra diverse Weltanschauung, ecc.), l'articolo si dipana presentando metodi dell'intelligenza artificiale applicati a un tema squisitamente culturale quale l'intelligence stessa, evidenziando per quest'ultima le problematiche e le "trappole" culturali, tra cui i *cognitive bias*, nei quali i suoi operatori possono incappare. Lo scritto non vuole caratterizzarsi come un contributo di stampo esclusivamente teorico ma anche pratico. Per questo motivo la parte conclusiva dell'articolo è dedicata a presentare gli sforzi recenti fatti dalla Commissione Europea in materia di finanziamento alla ricerca in settori di supporto alla cultural intelligence, fornendo una rapida panoramica di alcuni progetti di ricerca nei quali l'autore e la sua equipe sono coinvolti.

[4] Prigogine & Stengers (1981).

2. L'attività di cultural intelligence nei conflitti militari

La cultural intelligence è indispensabile «per determinare, valutare, ipotizzare gli sviluppi sia nel presente che nel futuro, nonché per individuare eventuali minacce e le necessarie contromisure»[5]. Su questa base è possibile affermare che un certo grado di *cultural awareness* sia necessario per sviluppare una piena *situational awareness*. Va ricordato come un'insufficiente conoscenza del contesto culturale locale sia stata tra le cause principali di alcune delle più fallimentari campagne condotte dagli Stati Uniti. Le spedizioni in Afghanistan e in Iraq, inaugurate rispettivamente nel 2001 e nel 2003, sono particolarmente significative in questo senso, in quanto in entrambi i casi ad una rapida serie di successi iniziali è seguita una lunga fase di occupazione e ricostruzione, pesantemente ostacolata dalla mancanza di cultural awareness da parte del personale militare della coalizione[6].

In Afghanistan l'incapacità di comprendere a fondo le strutture portanti della società e della cultura afghana pregiudicò notevolmente il tentativo della coalizione di guadagnarsi il rispetto e la fiducia della popolazione locale. Come ammesso più tardi dal generale di brigata David Fraser, allora a capo dell'International Security Assistance Force (ISAF), l'errore più grande fu quello di dare eccessivo peso alla cartina geografica quando invece sarebbe stato necessario soffermarsi sulla mappa tribale del paese[7].

Lo stesso sbaglio fu ripetuto in Iraq in seguito alla decapitazione del governo baathista. Numerosi marine americani di ritorno dall'Iraq lamentarono un'insufficiente preparazione riguardo a elementi chiave della cultura irachena. Ad esempio il fatto che i militari ignorassero totalmente il linguaggio dei gesti locale ebbe conseguenze spesso fatali sia per le truppe che per la popolazione. Basti pensare ai possibili effetti di un'errata interpretazione del gesto americano di stop (braccio teso con palmo della mano rivolto in avanti) – che in Iraq ha significato opposto di benvenuto – nel contesto di un posto di blocco[8]. A livello operativo, la limitata cultural awareness delle forze della coalizione impedì l'individuazione in tempi rapidi del principale sistema di trasmissione delle informazioni esistente nella società irachena, vale a dire la comunicazione orale. Senza la possibilità di instaurare legami personali con i cittadini iracheni, preclusa ai soldati per ragioni di sicurezza, una simile mancanza complicò

[5] Vivaldi (2014).
[6] Delp (2008).
[7] Spencer (2010).
[8] Mc Fate *"op. cit."*

notevolmente il tentativo di influenzare l'opinione pubblica locale così come la raccolta di intelligence da fonti umane (HUMINT)[9].

3. Cultural intelligence nella lotta al terrorismo

Le spedizioni militari in Afghanistan e in Iraq fanno parte di una campagna militare più ampia coordinata da Stati Uniti e Regno Unito e meglio nota come «guerra al terrorismo». Uno degli aspetti maggiormente enfatizzati di questo conflitto è la sua natura ideologica e di scontro tra insiemi di valori e credenze tra loro inconciliabili. Una battaglia il cui esito dipende non soltanto dalla sconfitta fisica dell'avversario ma anche dalla capacità di «vincere i cuori e la mente» dell'opinione pubblica internazionale e, in particolare, della *ummah* musulmana. In questo senso, le recenti missioni in Paesi a maggioranza islamica offrono alcune importanti lezioni riguardo alle potenzialità della cultural intelligence quale strumento di legittimazione. Una di queste riguarda l'impossibilità di ricostruire una società ignorando le norme, i valori e gli interessi su cui essa era precedentemente fondata. Tenere a mente le peculiarità della cultura locale è fondamentale per la ricostruzione delle istituzioni di un Paese così come per la lotta alle forze che si oppongono a questo processo. Sia in Afghanistan che in Iraq una maggiore cultural awareness da parte dei militari della coalizione avrebbe permesso di contrastare più facilmente le insurrezioni sviluppatesi in seno alle missioni, le quali affondavano le proprie radici nel contesto culturale locale[10].

Nel corso degli ultimi anni sono stati numerosi i casi in cui gruppi jihadisti sono entrati in conflitto sulla base di questioni attribuibili alla loro cultura di riferimento. La strage perpetrata nel 2004 in un istituto scolastico di Beslan, in Ossezia, è particolarmente emblematica sotto questo punto di vista. Il fatto che l'attentato ricevette l'apprezzamento di alcuni gruppi nazionalisti e islamisti ceceni ma fu esplicitamente condannato da altri, dimostra chiaramente come norme culturali locali e globali possano arrivare a scontrarsi in seno ad un unico movimento[11]. Un altro caso rilevante riguarda la recente disputa scoppiata tra la leadership di al Qaeda e quella dello Stato Islamico. La prima ha ripetutamente messo in dubbio la figura di Abu Bakr al Baghdadi, leader dell'ISIS, quale legittimo califfo[12] e tacciato lo Stato Islamico di arroganza e empietà per via dei metodi

[9] Mc Fate "*op. cit.*"
[10] Kilcullen (2014).
[11] Kilcullen "*op. cit.*"
[12] Styszynski (2014).

utilizzati[13]. A queste critiche alcuni pensatori vicini all'ISIS hanno replicato accusando al Qaeda di violare regolarmente la Sharia su questioni di carattere religioso e di stringere alleanze con attori considerati infedeli[14]. Anche da questo caso emerge la natura ideologica e culturale della disputa e, in particolare, il suo legame con due modi diversi di interpretare i valori contenuti nel Corano.

Se, da un lato, non è facile prevedere ciò che simili fratture possono comportare per il futuro del movimento jihadista, è chiaro come l'analisi delle dinamiche culturali che vi fanno da sfondo possa mettere i servizi di intelligence in una posizione di relativo vantaggio rispetto ai gruppi coinvolti. Quest'aspetto è emerso con particolare evidenza durante la lunga caccia a Osama Bin Laden, la cui cattura fu notevolmente ostacolata dal gap culturale esistente tra agenzie di intelligence e la popolazione delle aree in cui Bin Laden era nascosto. Una della maggiori conseguenze di questo gap fu la difficoltà di reclutare informatori tra gli abitanti della regione al confine tra Afghanistan e Pakistan, gli unici in grado di comprendere a fondo le strutture di potere esistenti nei villaggi e di fornire dettagli utili alla cattura dello sceicco del terrore. Le circa tre milioni di persone concentrate nelle aree tribali finirono per creare un vero e proprio muro intorno al leader di al Qaeda che sia l'esercito che i servizi segreti pachistani e la CIA furono a lungo incapaci di penetrare[15]. Il problema fu ben riassunto dal Vice Ammiraglio John Scott Redd, ai tempi a capo del National Counterterrorism Center (NCTC), quando, ad un reporter che gli chiedeva un commento sulle avanzate tecnologie di sorveglianza in possesso dei servizi segreti americani, rispose che ne avrebbe fatto volentieri a meno in cambio di tre valide fonti umane[16].

4. Terrorismo jihadista nell'era digitale: il ruolo della cyber intelligence

Negli ultimi anni, anche grazie al Web, l'epicentro dell'attività terroristica si è progressivamente spostato dall'organizzazione ai singoli individui con la prima relegata ad un ruolo di ispirazione ideologica e indirizzamento strategico piuttosto che di natura operativa. Attraverso Internet aspiranti jihadisti di tutto il mondo possono accedere in maniera relativamente semplice ad un'enorme collezione di materiale propagandistico di matrice islamista e sviluppare il *know-how* necessario

[13] Habeck (2014).
[14] Fairchild (2014).
[15] Burke (2011).
[16] Delp (2008).

per mettere in pratica un attacco. Questa dinamica ha facilitato la nascita di un movimento globale che, seppur fisicamente non connesso, è in grado di ispirare e guidare i propri seguaci nella realizzazione di attentati. Un movimento che per via della sua natura fluida e decentralizzata è stato descritto da Marc Sageman con la celebre definizione di «*leaderless jihad*»[17].

Se, da un lato, la pervasività delle nuove tecnologie ha contribuito a rafforzare terroristi e jihadisti, dall'altro questa li ha resi più vulnerabili all'armamentario della cyber intelligence. Non a caso Osama bin Laden non utilizzava le tecnologie dell'informazione per timore di essere intercettato e localizzato, una strategia che gli consentì di sfuggire alla cattura per dieci anni. Lo Stato Islamico si è dimostrato meno prudente sotto questo punto di vista, determinato a sfruttare al massimo i vantaggi derivanti dall'utilizzo a fini propagandistici dei social media e delle più moderne tecnologie informatiche. Alcune delle tattiche adoperate dall'ISIS in seguito alla proclamazione del Califfato nell'estate del 2014 paiono il frutto di una sofisticata strategia di comunicazione avente tra gli altri due obiettivi: quello di diffondere il più possibile il messaggio jihadista e, al tempo stesso, fare apparire l'organizzazione più forte di quanto effettivamente non sia[18]. Singolare è stata, in tal senso, la creazione di un'applicazione per smartphone chiamata '*The Dawn of Glad Tidings*' che, oltre ad informare l'utente sulle ultime novità riguardanti lo Stato Islamico, permette al gruppo di ritrasmettere periodicamente i propri messaggi attraverso gli account Twitter di coloro che hanno scaricato l'applicazione[19]. L'idea è di amplificare quella che è in realtà la voce di pochi militanti al punto da farla risuonare come il grido di un movimento in una fase di crescita esponenziale. Un simile risultato è stato perseguito tramite l'utilizzo, sempre su Twitter, di *bot* e *hashtag* popolari. Una frazione dei tweet riconducibili allo Stato Islamico proviene da computer che sono stati infiltrati dai militanti dell'organizzazione e che sono ora sfruttati per diffondere in modo automatico la propaganda dell'organizzazione. I tweet si agganciano spesso a hashtag specifici dell'IS (es. #AllEyesOnISIS) o relativi a particolari eventi di pubblico interesse (es. #WorldCup2014), a dimostrazione di come il gruppo ambisca ad intensificare il flusso della propria propaganda e, inserendola all'interno di conversazioni in corso, accrescerne la visibilità[20].

---

[17] Sageman (2008).
[18] Berger (2014).
[19] CBSDC (2014).
[20] Levy (2014).

Grazie alle tecnologie comunemente associate al Web 2.0, chiunque lo desideri può oggi giocare un ruolo importante all'interno del movimento jihadista. Ciò è testimoniato dalla sempre più accentuata componente online del processo di radicalizzazione. E' attraverso l'uso di piattaforme come Facebook, Twitter e YouTube che passa sempre più spesso il percorso di adesione individuale al sistema ideologico jihadista[21]. E' infatti qui che molti giovani entrano in contatto con la retorica e i simboli della cultura jihadista, un incontro che può portare ad una radicalizzazione più o meno graduale delle proprie credenze e, in alcuni casi, varcare il confine tra mondo virtuale e mondo reale. L'uso dei social media ha inoltre permesso alla macchina propagandistica dello Stato Islamico di autoalimentarsi, sfruttando il contributo di migliaia di utenti sparsi in tutto il mondo: simpatizzanti che hanno deciso di partecipare in maniera indipendente alla campagna jihadista rilanciando a loro volta il materiale creato dall'organizzazione. Questa componente individuale è ben presente nel processo di disseminazione della propaganda dello Stato Islamico così come di altri contenuti diretti a supportarne gli obbiettivi. Secondo un report prodotto dal Centro Internazionale per lo Studio delle Radicalizzazione (ICSR), molti dei *foreign fighter* impegnati al momento in Siria tendono a ricevere informazioni sul conflitto non attraverso i canali messi a disposizione dai rispettivi gruppi, come, ad esempio, gli account ufficiali, bensì tramite un'ampia gamma di simpatizzanti, che non hanno alcun legame con i gruppi militanti e che sono spesso basati in Occidente. Nonostante molti di questi 'disseminatori' non abbiano mai messo piede in Siria, si ritiene che abbiano un impatto considerevole sul modo in cui il conflitto viene percepito da parte di coloro che ne sono direttamente coinvolti[22]. Tale influenza è dovuta alla capacità di queste figure di accedere ad un maggior numero di fonti e di fornire una visione più ampia rispetto ai singoli gruppi attivi sul territorio, diretta conseguenza della loro natura di freelance ma anche della continua interazione con i rispettivi *follower*[23]. Tra questi disseminatori uno dei più autorevoli, conosciuto come Shami Witness, aveva accumulato un seguito di ben 17,000 utenti, prima di essere individuato ed arrestato nella periferia di Bangalore, in India, nel dicembre del 2014[24]. Inizialmente ritenuto da esponenti dell'intelligence e della comunità accademica come una pedina chiave della macchina ideologica/propagandistica del Califfato[25], Shami Witness si è

[21] COPS (2014).
[22] Carter *et al*. (2014).
[23] Carter *et al*. "*op. cit.*"
[24] Spencer (2014).
[25] Carter *et al*. (2014).

rivelata essere la maschera virtuale di un giovane privo di legami diretti con l'organizzazione jihadista che, oltre a trascorrere le giornate divulgando materiale estremista sul Web, si dilettava ad indossare camicie hawaiane, mangiare pizza e guardare film di supereroi[26]. Il colossale fraintendimento del ruolo di semplice 'jihadista da poltrona' svolto da Shami Witness è emblematico delle nuove dinamiche interne al movimento jihadista globale ma anche dei rischi associati alla cyber intelligence: un'attività che non può prescindere dal connubio tra raccolta di informazioni online e comprensione del contesto socio-culturale in cui esse vengono scambiate.

Non va però dimenticato come la digitalizzazione della comunicazione jihadista abbia aperto prospettive importanti anche per i servizi di sicurezza. L'enorme quantità di materiale islamista attualmente presente sul Web offre all'intelligence una vetrina straordinaria sull'ecosistema del fondamentalismo attraverso la quale è possibile studiare il comportamento di singoli attori ma anche i contesti sociali e culturali in cui essi operano. Sotto questo profilo, i social media rappresentano un mezzo straordinario per la produzione di cultural intelligence, l'utilizzo del quale richiede tuttavia la capacità di gestire e analizzare il mare di contenuti accessibili online e, allo stesso tempo, comprendere gli effetti di tali contenuti sui 'cuori e le menti' di coloro che ne fruiscono[27].

5. Il rapporto tra cultural e cyber intelligence tra opportunità e sfide

Quando ancora la guerra civile in Siria non si era evoluta in un conflitto su scala regionale Phillip Smyth, un analista autodidatta statunitense allora ventisettenne, passava le nottate ad osservare le attività di diversi gruppi militanti sciiti sui social media. Fin da bambino Smyth aveva sviluppato un forte interesse per la cultura libanese che lo aveva portato nel corso degli anni a compiere un viaggio in Libano, ad imparare l'arabo e a studiare quasi ossessivamente i gruppi religiosi attivi nel paese. E' però da casa sua, a Washington D.C., che Smyth portava avanti il suo hobby, chattando con i militanti sui forum Internet e costruendo un enorme database composto da tweet, post su Facebook e altro materiale proveniente dal Web[28]. Uno degli aspetti che più attirarono la sua attenzione fu la musica pop religiosa prodotta da alcuni di questi gruppi. Analizzando i testi di diverse canzoni, Smyth si rese conto di come un numero crescente di queste avesse cominciato a promuovere un messaggio di natura militante, condito da

[26] Sharkov (2014).
[27] Zanasi (2014).
[28] Cambanis (2014).

esplicite minacce nei confronti dei gruppi ribelli siriani. Smyth notò inoltre come i brani fossero spesso cantati in un dialetto iracheno della lingua araba, testimonianza di come la musica fosse stata appositamente creata per il pubblico iracheno[29]. Smyth ne dedusse che alcune milizie sciite irachene erano pronte a prender parte alla guerra civile siriana al fianco dell'esercito di Bashar al-Assad, conclusione che si rivelò corretta e che fu in seguito ripresa dai media e dal governo americano come prova della dimensione regionale ormai assunta dal conflitto[30].

La lezione chiave che ci giunge dalla vicenda di Phillip Smyth riguarda la necessità che i servizi di intelligence diventino più abili a seguire la cultura nelle varie forme in cui essa si manifesta[31]. Grazie a Internet e ai social media questo obiettivo è ora raggiungibile ad un costo estremamente inferiore che in passato. Fino a pochi anni fa, l'analisi della cultura di un gruppo militante straniero richiedeva una quantità di risorse che nemmeno le grandi agenzie di intelligence erano spesso in grado di garantire. Oggi non è più così e le dinamiche culturali che determinano il comportamento di particolari attori possono essere studiate attraverso il flusso di informazioni liberamente accessibili online. Ciò non significa che chiunque sia in possesso di una connessione ad Internet possa offrire un contributo valido al lavoro di monitoraggio svolto dai servizi di sicurezza. Un'efficace analisi di open source intelligence richiede avanzate competenze linguistiche e una profonda conoscenza dei gruppi oggetto di studio. Tuttavia, il problema principale sta nella difficoltà di individuare le informazioni utili all'interno della valanga di dati disponibili online. Tale dinamica può sfociare nell'*information overload*, fenomeno in cui la capacità dell'analista di distinguere intelligence critica dal rumore viene pregiudicata dal volume eccessivo di informazioni che questo si trova a dover gestire. In questo senso, la vera sfida per i servizi di intelligence consiste nello sviluppare la capacità di processare e monitorare quasi in tempo reale i milioni di contenuti multimediali che passano ogni giorno attraverso il Web[32].

Una soluzione al problema dell'information overload è fornita dall'utilizzo di tecniche di *data* e *text mining*. Queste metodologie permettono di analizzare in modo automatico vari volumi di dati - siano essi di natura strutturata o non strutturata, quantitativa o qualitativa – e produrne una sintesi che può essere compresa con maggiore rapidità e

[29] Smyth (2013).
[30] Cambanis (2014).
[31] Cambanis "*op. cit.*".
[32] Cambanis "*op. cit.*".

semplicità dall'analista allo scopo di generare intelligence[33]. Simili tecnologie possono essere particolarmente utili per la produzione di cultural intelligence in funzione antiterrorismo. Una fetta significativa del materiale di matrice jihadista attualmente in circolazione online è scritta in arabo o in altre lingue non occidentali. Per arrivare a decifrare in modo corretto questo materiale è necessaria una conoscenze di queste lingue e una comprensione del contesto culturale di riferimento, competenze che mancano di frequente anche alle agenzie di intelligence più potenti[34]. L'uso di software con funzionalità di text mining permette di ovviare almeno in parte al problema, consentendo l'analisi di grandi quantità di dati testuali anche in lingue esotiche e sconosciute ai più. Il text mining rende possibile, ad esempio, il monitoraggio delle comunità virtuali in cui hanno luogo le conversazioni tra jihadisti. Tramite tali tecniche gli analisti possono infatti ricostruire il contesto comunicativo e le relazioni esistenti tra documenti differenti, rilevando riferimenti a temi di interesse, come questi vengono trattati e quali impressioni essi generano nel lettore[35].

L'utilizzo di tecnologie deputate all'analisi automatizzata di dati offre senza dubbio notevoli benefici in relazione agli attuali requisiti del lavoro di intelligence. Attraverso l'automatizzazione di funzioni che andrebbero altrimenti compiute manualmente, questi strumenti hanno il pregio di aiutare analisti ed investigatori ad individuare gli aspetti a cui dare priorità e su cui applicare il proprio giudizio umano[36]. Tuttavia è importante sottolineare come la tecnologia non vada scambiata per la soluzione di tutte le problematiche affrontate oggi dalla comunità di intelligence. Attribuendo alla tecnologia qualcosa in più di un ruolo di supporto l'analista corre il rischio di formulare conclusioni errate che, specialmente in ambito di antiterrorismo, possono avere effetti estremamente nefasti[37].

Alcuni degli errori più comuni tra gli analisti di intelligence sono di natura cognitiva, frutto della tendenza inconscia degli esseri umani a semplificare il processo decisionale in situazioni di complessità e incertezza. L'utilizzo di queste 'scorciatoie mentali', chiamate *cognitive bias*, può indurre deviazioni di giudizio basate su fattori quali memoria, esperienza, istruzione, background culturale e credenze politiche o ideologiche[38]. Un uso improprio della tecnologia può favorire il verificarsi di determinati bias o contribuire in modo significativo ad ampliarne gli

---

[33] Zanasi (2007).
[34] Zanasi (2009).
[35] Zanasi *"op. cit."*
[36] De Rosa (2004)
[37] De Rosa *"op. cit."*
[38] Heuer (1999).

effetti. Software di data mining con funzionalità di 'clustering', ad esempio, permettono di suddividere automaticamente insiemi di dati in varie classi (definite 'cluster') in relazione al loro grado di somiglianza. Se utilizzata correttamente, questa tecnica può essere sfruttata, tra le altre cose, per tracciare il profilo di potenziali terroristi a partire da materiale raccolto da siti Web jihadisti[39]. Tuttavia un utente inesperto che commetta errori come, ad esempio, mantenere le impostazioni di default del software utilizzato per l'analisi, rischierebbe di ottenere cluster errati, potenzialmente in grado di mascherare le differenze interne al gruppo di riferimento. Questa dinamica potrebbe portare l'utente a incappare in un bias cognitivo noto come '*out-group homogeneity*' che consiste nella tendenza a percepire i membri del proprio gruppo come maggiormente diversi gli uni dagli altri rispetto ai membri di altri gruppi. Il manifestarsi di questo bias può indurre l'analista a sopravvalutare somiglianze tra oggetti (per esempio persone) appartenenti allo stesso cluster, una dinamica che può impattare negativamente sul prodotto di intelligence finale.

La prevenzione di questi errori è considerata un obiettivo sempre più importante all'interno della comunità di intelligence. Attraverso il programma di finanziamento FP7, la Commissione Europea ha di recente allocato diversi milioni di euro per la realizzazione di un progetto di ricerca – RECOBIA[40] (REduction of Cognitive Biases in Intelligence Analysis), di cui l'autore è partner – il cui scopo è migliorare la qualità delle analisi di intelligence attraverso la mitigazione degli effetti negativi prodotti dai bias cognitivi. Uno dei risultati chiave del progetto, il cui completamento è previsto ad inizio 2015, riguarda proprio il doppio ruolo giocato dalle tecnologie dell'informazione quali soluzioni e allo stesso tempo possibili cause di determinati bias cognitivi. A testimonianza del crescente interesse dei policy-maker europei per l'esplorazione di nuovi modi di applicare la tecnologia al settore dell'intelligence, vale la pena ricordare un altro progetto di ricerca di cui l'autore è partner e finanziato dalla Commissione Europea. Conosciuto con l'acronimo di LEILA[41] (Law Enforcement Intelligence Learning Applications), il progetto ha anch'esso lo scopo di ottenere performance migliori a livello di analisi di intelligence. Tuttavia, invece che agire direttamente sulla fase di analisi, LEILA ambisce a migliorare il processo di addestramento degli analisti, proponendo un'innovativa metodologia incentrata sull'utilizzo di particolari videogiochi, noti come *'serious game'*, a scopo formativo. Come metodologia di

[39] Last *et al.* (2003).
[40] https://www.recobia.eu/
[41] http://leila.fvaweb.eu/

apprendimento, i serious game permettono di simulare situazioni reali e favoriscono lo sviluppo di abilità e conoscenze altrimenti difficili da acquisire. Per questo, il loro utilizzo sta crescendo di popolarità non solo in ambito di sicurezza ma anche in settori come l'istruzione, la sanità e il business.

I progetti RECOBIA e LEILA sono indicativi del legame ormai sempre più stretto tra cyber e cultural intelligence. L'insieme di valori, norme e istituzioni che formano una cultura ha un impatto profondo su come le persone percepiscono il mondo esterno e, in quanto tale, è in grado di favorire o ostacolare il manifestarsi di particolari bias cognitivi. L'utilizzo della tecnologia dell'informazione in fase di addestramento così come di analisi di intelligence, può quindi risultare inefficace e perfino dannoso in mancanza di un'adeguata comprensione del contesto socio-culturale di riferimento. Al tempo stesso è vero come un'analisi sistematica delle attività online di un determinato attore permetta di svelare più facilmente le dinamiche culturali che ne influenzano il comportamento. E' quindi in questa direzione che i servizi di sicurezza dovranno indirizzare i propri sforzi futuri: nel comprendere e sfruttare appieno le opportunità create dalla 'nuova alleanza' tra cyber intelligence e cultural intelligence.

6. Conclusioni

L'analisi della cultura altrui è un fenomeno tutt'altro che recente in ambito militare e di sicurezza. Tuttavia nel corso degli ultimi anni essa è stata soggetta ad un processo di profonda trasformazione. Ad essere cambiata non è soltanto l'importanza della cultural intelligence ma anche gli strumenti attraverso cui questa può essere oggi perseguita. La diffusione delle tecnologie dell'informazione ha portato alla nascita di un singolare binomio tra cultural intelligence e cyber intelligence. Da un lato l'attuale guerra al terrorismo ha assunto un carattere sempre più marcatamente ideologico. Dall'altro essa vede nel Web uno dei suoi principali campi di battaglia. All'interno di un simile conflitto cyber e cultural intelligence non possono che giocare un ruolo complementare: la prima facendo sì che le informazioni utili disponibili online non vengano ignorate, la seconda assicurando che queste vengano interpretate nel modo corretto. Se il percorso di integrazione tra queste discipline presenta ancora numerose insidie, mai prima d'ora cultura e tecnologia sembrano essere state così vicine.

Bibliografia[42]

Berger, J. (2014). *How ISIS Games Twitter*. «The Atlantic», 16 giugno. http://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/

Burke, J. (2011). *Osama bin Laden: the long hunt*. «The Guardian», 2 Maggio. http://www.theguardian.com/world/2011/may/02/osama-bin-laden-long-hunt

Cambanis, T. (2014). *The jihadi hunters*, «The Boston Globe», 2 ottobre 2014 http://www.bostonglobe.com/ideas/2014/10/02/the-jihadi-hunters/tTC2t6UNIyzlioSoGBs5VO/story.html

Carter, J.A., Maher, S. & Neumann, P.R. (2014). *#Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks*. International Centre for the Study of Radicalization. http://icsr.info/wp-content/uploads/2014/04/ICSR-Report-Greenbirds-Measuring-Importance-and-Infleunce-in-Syrian-Foreign-Fighter-Networks.pdf

Coles, J.P. (2005). *Cultural Intelligence and Joint Intelligence Doctrine*, «Joint Operations Review», Joint Forces Staff College, http://www.au.af.mil/au/awc/awcgate/ndu/jfsc_cultural_intelligence.pdf

Community Oriented Policing Services (COPS) (2014). *Online Radicalization to Violent Extremism*, http://www.theiacp.org/portals/0/pdfs/RadicalizationtoViolentExtremismAwarenessBrief.pdf

Delp, B.T. (2009). *Ethnographic Intelligence (ETHINT) and Cultural Intelligence (CULINT): Employing under-utilized strategic intelligence gathering disciplines for more effective diplomatic and military planning*. IIIA Technical Paper 08-02. Institute for Infrastructure and Information Assurance, James Madison University. http://www.jmu.edu/iiia/wm_library/CulturalIntelligenceTR08-02.pdf

De Rosa (2004). *Data Mining and Data Analysis for Counterterrorism*. Washington D.C.: Center for Strategic and International Studies

Fairchild (2014). *Abu Bakr al Baghdadi: From Terrorist Commander to Religious Icon*. «*Blind* Eagle: Periodic Strategic Analysis on National Security Issues», 26 settembre 2014 http://www.blindeagle.info/2014/09/26/abu-bakr-al-baghdadi-from-terrorist-commander-to-religious-icon/

[42] La data di ultimo accesso alle pagine web citate è il 26 gennaio 2015.

Heuer, R.J. (1999). *Psychology of Intelligence Analysis*. Central Intelligence Agency (CIA) https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/PsychofIntelNew.pdf

ISIS Launches Twitter App For Android Phones (2014). «CBSDC», 17 giugno, http://washington.cbslocal.com/2014/06/17/isis-launches-twitter-app-for-android-phones/

Last, M., Elovici, Y., Shapira, B., Zaafrany, O. & Kandel, A. (2003). *Using Data Mining Techniques for Detecting Terror-Related Activities on the Web*. ECIW Proceedings, 271-280

Levy, R. (2014). *ISIS Tries to Outwit Social Networks*, «Vocativ», 17 giugno, http://www.vocativ.com/world/syria-world/isis-tries-outwit-social-networks/

Kilcullen, D.J. (2004). *Countering Global Insurgency*. «Small Wars Journal». smallwarsjournal.com/documents/kilcullen.pdf

McFate, M. (2005). *The Military Utility of Understanding Adversary Culture*, Office of Naval Research, http://www.au.af.mil/au/awc/awcgate/jfq/1038.pdf

Prigogine, I. & Stengers, I. (1981). *La Nuova Alleanza. Metamorfosi della scienza*. Torino:Giulio Einaudi Editore

Sageman, M. (2008). *Leaderless Jihad: Terror Networks in the Twenty-First Century.* Philadelphia: University of Pennsylvania Press

Sharkov, D. (2014). *Major ISIS Twitter Propagandist Unmasked As Pizza-Loving Indian Businessman. «Newsweek»,* 12 Dicembre http://www.newsweek.com/major-isis-twitter-propagandist-unmasked-pizza-loving-bangalore-businessman-291414

Smyth, P. (2013). *Hizballah Cavalcade: The Songs of Liwa'a Abu Fadl al-Abbas: Militant Iraqi Shia Music & Syria*. «*Jihadology*», 3 luglio http://jihadology.net/2013/07/03/hizballah-cavalcade-the-songs-of-liwaa-abu-fadl-al-abbas-militant-iraqi-shia-music-syria/

Spencer, E. (2010), *Solving the People Puzzle: Cultural Intelligence and Special Operations Forces.* Toronto: Dundurn Press

Spencer, R. (2014). *Isil tweeter 'ShamiWitness' arrested in India*, «The Telegraph», 13 dicembre http://www.telegraph.co.uk/news/worldnews/islamic-state/11292412/Isil-tweeter-ShamiWitness-arrested-in-India.html

Vivaldi, A. (2014). *Cultural Intelligence: Geopolitica, Intelligence e Scienze Umane*. https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/10/Cultural-intelligence-Alessandro-Vivaldi.pdf

Zanasi, A. (2007). *Text Mining and its Applications to Intelligence, CRM and KM*. Southampton, Boston. WIT Press.

Zanasi, A. (2009). "Virtual Weapons for Real Wars: Text Mining for National Security" in Corchado, E., Zunino, R. Gastaldo, P. & Herrero, A. (eds.), *Proceedings of the International Workshop on Computational Intelligence in Security for Information Systems CISIS'08*. Verlag Berlin Heidelberg: Springer

Zanasi, A. (2014). *L'Intelligence e la battaglia delle idee*. «Airpress». Settembre 2014.

FrancoAngeli
Scienza Politica
e Relazioni Internazionali

Cyber Warfare 2014

La quinta Conferenza Nazionale sulla Cyber Warfare si è svolta con una nuova formula, in due edizioni: la prima, "Lo Sviluppo delle Armi Cibernetiche" (Roma, 11 ottobre 2014), dedicata ad un approccio strategico e la seconda, "L'utilizzo della Cyber Intelligence per la Difesa del Business" (Milano 13 ottobre 2014), dedicata a problematiche economiche. Il progressivo aumento della frequenza di attacchi informatici sempre più sofisticati e dirompenti rende prioritaria l'introduzione di innovazioni politico-strategiche, organizzative, tecnologiche e culturali affinché i decisori politici ed aziendali siano costantemente aggiornati e pronti ad interagire in tempi brevissimi garantendo, come già affermato nelle scorse edizioni, una stretta collaborazione tra mondo civile, militare e accademico. L'evento è stato ideato dal Centro Interdipartimentale Studi Strategici, Internazionali e Imprenditoriali (CSSII) dell'Università di Firenze, dall'Istituto per gli Studi di Previsione (ISPRI), dal Centro Studi Difesa e Sicurezza (CESTUDIS) e dal Centro di Ricerca di Cyber Intelligence and Information Security (CIS) de "La Sapienza" di Roma, d'intesa con Maglan Group – Information Defense and Technologies. La Conferenza ha avuto l'adesione del Presidente della Repubblica e sua Medaglia di Rappresentanza ed il patrocinio di Senato della Repubblica, Ministero della Difesa e Ministero dello Sviluppo Economico.

Umberto Gori, professore emerito dell'Università degli Studi di Firenze, è presidente del Centro interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CSSII) e direttore dell'Istituto per gli Studi di Previsione e le Ricerche Internazionali (ISPRI).

Serena Lisi è docente a contratto di Analisi e Pianificazione delle Operazioni di Pace all'Università degli Studi di Firenze.

MAGLAN
Information Defense & Intelligence

FrancoAngeli
La passione per le conoscenze

ISBN 978-88-917-1425-1