Social media intelligence e sicurezza nazionale
La raccolta informativa sui social media

di Stefano Mele, Matteo Faini e Carmine America

Abstract

Il poderoso, recente, sviluppo dei social media offre alle agenzie di intelligence nuove opportunità nell'analisi delle informazioni per la sicurezza nazionale. Al contempo, però, il grande volume di dati prodotto da tali sistemi di comunicazione pone non pochi problemi riguardo alla corretta ed efficiente raccolta informativa. Come individuare, quindi, all'interno del vasto flusso di dati le informazioni rilevanti per l'intelligence distinguendole da quelle inutili o addirittura fatte circolare per disinformare? Secondo gli autori ciò potrà avvenire soprattutto grazie alla creazione di unità 'joint' nelle quali analisti delle diverse agenzie – anche tramite una proficua inter-relazione con il settore privato detentore di know-how strategico – possano mettere sinergicamente a fattor comune le loro diverse specializzazioni.

Profilo autori

Stefano Mele è avvocato specializzato in Diritto delle Tecnologie, Privacy, Sicurezza delle Informazioni e Intelligence. Lavora a Milano come 'of Counsel' di Carnelutti Studio Legale Associato. È socio fondatore e Partner del Moire Consulting Group ed è Presidente del 'Gruppo di lavoro sulla cyber-security' della Camera di Commercio Americana in Italia. È coordinatore dell'Osservatorio InfoWarfare e Tecnologie emergenti dell'Istituto Italiano di Studi Strategici 'Niccolò Machiavelli' ed è inoltre docente e direttore di ricerca presso istituti di formazione e di ricerca del Ministero della Difesa italiano e della NATO. Nel 2014, la NATO lo ha inserito nella lista dei suoi 'Key Opinion Leaders for Cyberspace Security' e la rivista Forbes lo ha inserito tra i 20 migliori 'Cyber Policy Experts' al mondo da seguire in Rete.

Matteo Faini ha recentemente completato un PhD in Politics all'Università di Princeton, con una tesi sui rapporti tra agenzie di intelligence e decisori politici. È research fellow nell'International Security Program al New America e Lecturer in Politics all'Università di Venezia, Ca' Foscari. È autore, tra gli altri, di *The US Government and the Italian Coup Manqué of 1964: The Unintended Consequences of Intelligence Hierarchies* (di prossima pubblicazione in *Intelligence and National Security*).

Carmine America si occupa di sicurezza in una multinazionale italiana del settore Difesa e Aerospazio. Ha maturato esperienze professionali presso lo Stato maggiore della Marina, la commissione Disarmo e sicurezza internazionale dell'Assemblea generale Onu ed i principali think tank di Washington DC. È socio del Centro Studi Americani e collabora con le riviste Formiche e Airpress.

Keyword

social media, signal-to-noise ratio

Prima di andare ad attaccare nel maggio 2015 una manifestazione in Texas dedicata alle vignette satiriche su Maometto, Elton Simpson ha annunciato il suo intento su Twitter, lanciando l'hashtag #Texasattack. Poco dopo, insieme ad un complice, ha indossato un giubbotto antiproiettile ed ha guidato la sua macchina fino al sito della manifestazione, dove ha maldestramente cercato di sparare ai partecipanti. Sia lui sia il complice sono morti sotto i colpi di un singolo poliziotto texano, armato di una semplice pistola, senza che vi fossero altre vittime.

Elton Simpson era noto alle autorità. Era stato condannato cinque anni prima per aver mentito riguardo al suo progetto di unirsi ad al-Shabaab in Somalia e i suoi frequenti scambi su Twitter con membri dello Stato Islamico in Iraq e Siria venivano monitorati. Subito prima dell'attacco, l'FBI aveva mandato un allarme alle autorità locali, ma non sembra che il messaggio sia arrivato in tempo utile a consentire di prendere ulteriori misure protettive.

Casi come quello di Simpson stanno diventando sempre più comuni. Anziché nascondere le proprie simpatie per gruppi terroristi, se non addirittura la propria appartenenza e i propri progetti di attentati, molti ne parlano apertamente sui social media. Dopo un attentato, ci si accorge che per impedirlo sarebbe bastato monitorare quanto questi aspiranti terroristi pubblicavano su Internet.

Purtroppo non basta aggiungere Al Qaeda o lo Stato Islamico agli amici su Facebook per sventarne questo genere di progetti. Tuttavia, l'intelligence che si può raccogliere attraverso i social media, comunemente chiamata Social Media Intelligence o SOCMINT, sta diventando sempre più importante e non solo nella lotta al terrorismo. Questo articolo si limita a considerare l'utilizzo dei social media da parte delle agenzie di intelligence a fini di raccolta informativa, escludendo dunque altri usi possibili come la propaganda e non tratta delle importanti questioni etiche che esso solleva[1]. L'articolo prima analizza potenzialità e ostacoli della raccolta informativa sui social media. Poi propone qualche parziale soluzione dal punto di vista organizzativo, delle tecniche analitiche, e delle possibili collaborazioni con il settore privato.

In breve, l'articolo sostiene che i social media esasperino un vecchio problema della raccolta informativa, riducendo quello che in gergo si chiama *signal-to-noise ratio*, ossia la proporzione tra i segnali di genuino interesse e il mare di rumore e chiacchiericcio inutile e spesso ingannevole. Per navigare in questo 'mare insidioso' dei social media, le agenzie di intelligence hanno bisogno della bussola che solo altri tipi di intelligence, come HUMINT o SIGINT, sanno offrire. Solo così l'intelligence potrà battere la concorrenza di altre fonti informative a cui i decisori politici potrebbero altrimenti rivolgersi. Per massimizzare l'efficacia della raccolta informativa, diventa dunque importante creare unità in cui specialisti delle diverse intelligence lavorino fianco a fianco, sfruttando anche il rilevante flusso informativo proveniente dal settore privato. È il settore privato, infatti, che – soprattutto nell'ambiente 'cyber' – risulta detentore delle cosiddette informazioni di 'soglia', ovvero quelle relative alle tecniche operative, agli strumenti, alle tecnologie e spesso anche alle strategie adottate dai principali attori che operano attraverso il cyber-spazio[2].

Il valore e gli ostacoli della SOCMINT

Quali informazioni possono essere raccolte sui social media? Che valore hanno queste informazioni e come possono essere sfruttate dalle agenzie di intelligence? Come è facile intuire per un concetto introdotto solo quattro anni fa, la letteratura sulla SOCMINT è ancora in una fase embrionale e siamo ancora lontani dall'avere una risposta completa a queste domande.

Ad attirare l'attenzione degli studiosi verso il ruolo giocato dai social media furono soprattutto le proteste del movimento verde in Iran nel 2009 e, due anni dopo, le rivolte della Primavera araba e i quattro giorni di sommossa in Inghilterra nell'agosto 2011. Fu subito chiaro che Twitter e Facebook offrono una piattaforma istantanea su cui organizzarsi, coordinarsi e su cui raccontare le proprie gesta, facilitando l'azione collettiva di masse altrimenti disorganizzate.

Se da un lato i social media possono essere sfruttati da chi protesta contro governi più o meno democratici, dall'altro possono essere utilizzati dai governi stessi per raccogliere informazioni. Il valore di queste informazioni potrebbe sembrare a prima vista quasi illimitato. Sapere in anticipo dove si concentreranno i manifestanti può essere di grande aiuto per chi vuole contenere i disordini o reprimere il dissenso. Prima che scoppino le rivolte, il monitoraggio dei social media può consentire di capire quale sia lo stato dell'opinione pubblica, aiutando a prevedere le rivolte stesse. Monitorando poi gli account degli appartenenti a gruppi terroristici, alcuni dei quali sono molto attivi sui social media, si potrebbero controllare i canali di comunicazione, di propaganda, di reclutamento e addirittura di pianificazione degli attentati.

I sostenitori più entusiasti della SOCMINT, come Jane Harman, già membro del comitato di controllo sull'intelligence della Camera dei Rappresentanti americana e ora Presidente del Wilson Center for International Scholars, si spingono fino a sostenere che il valore dell'intelligence raccolta sui social media sarà maggiore rispetto a quella raccolta con metodi tradizionali come la HUMINT[3]. Sostiene la Harman che «per seguire le vicende in Ucraina alla CIA non serve una fonte all'interno del Ministro dell'Agricoltura russo», in quanto i resoconti migliori sono disponibili sui social media. La spia che origlia qualche frase ad un cocktail party apparterrebbe quindi al passato, destinata ad estinguersi come una creatura preistorica.

Si tratta evidentemente di un'esagerazione, ma sarebbe sbagliato liquidarla con una semplice alzata di spalle. Se, infatti, i decisori politici si convincessero che le agenzie di intelligence non offrono nulla di più rispetto a quello che essi stessi possono trovare sui social media, il rischio è che finiscano per basare le proprie decisioni su informazioni non verificate e in certi casi intenzionalmente fuorvianti. Trovandosi a competere con i social media per l'attenzione dei decisori politici, le agenzie di intelligence potrebbero vedersi incentivate a privilegiare la rapidità con cui trasmettono le proprie informazioni a scapito della loro accuratezza e autorevolezza[4]. Diventa dunque ancor più importante spiegare quali siano i limiti e gli ostacoli posti dalla SOCMINT.

L'ostacolo fondamentale è quello che gli studiosi di intelligence chiamano il basso *signal-to-noise ratio*: per ogni informazione utile rintracciabile sui social media vi sono migliaia e migliaia di informazioni inutili. Ogni segnale viene sommerso in una quantità spesso assordante di rumore.

Distinguere i segnali dal rumore è quanto mai difficile, per tre motivi: i falsi positivi, i falsi negativi e la disinformazione.

Si prenda ad esempio la lotta al terrorismo: su cento persone che manifestano la propria simpatia per lo Stato Islamico e per i suoi progetti di attentati, solo una frazione minuscola passerà effettivamente all'azione. In altre parole, il numero di falsi positivi, ossia di casi che sembrano essere di interesse, ma che in realtà non lo sono o lo sono solo in parte, è elevatissimo.

C'è anche il problema opposto: chi pianifica un attentato ha tutto l'interesse a non parlarne sui social media. È vero che il bisogno psicologico di pubblicità induce spesso queste persone a pubblicare più di quanto a loro converrebbe, ma, pur in mancanza di dati precisi, è ragionevole pensare che la maggior parte dei terroristi o aspiranti tali non sia così ingenuamente loquace. Oltre ai falsi positivi, dunque, gli analisti dovranno fronteggiare i falsi negativi: casi di interesse che non lanciano alcun segnale sui social media.

Conoscendo queste difficoltà analitiche, gli avversari delle agenzie di intelligence hanno tutto l'interesse ad esasperarle, inondando le agenzie con chiacchiericcio inutile ed intenzionalmente fuorviante. I social media hanno moltiplicato a dismisura l'opportunità di diffondere disinformazione, non solo da parte dei gruppi terroristi. Notizie false o fuorvianti vengono facilmente diffuse ad una rapidità prima impensabile, senza i controlli messi in atto dai media più tradizionali. Dopo tanti falsi allarmi, qualsiasi sistema di difesa finisce inevitabilmente per abbassare la guardia, offrendo l'opportunità di colpire.

Il basso *signal-to-noise ratio*, i falsi positivi, i falsi negativi e la disinformazione rendono molto difficile fare previsioni sulla base della SOCMINT, specie quando si tratta di prevedere eventi a cui partecipa un numero ristretto di persone, come nel caso di un attentato. Quando si tratta di eventi di massa, come una protesta, la SOCMINT, invece, diventa uno strumento più affidabile. Diffondere disinformazione è più difficile, ma non certo impossibile, quando essa riguarda centinaia di persone anziché una manciata. Inoltre, i falsi negativi e falsi positivi sono meno importanti. Una protesta non sarà sostanzialmente diversa nel caso in cui qualcuno che voglia parteciparvi poi non lo faccia (falsi positivi), oppure quando altri vi partecipano pur avendo detto di non voler partecipare o non avendo detto nulla (falsi negativi). Tuttavia, lo stesso non può certo dirsi nel caso di un attentato.

Nel prevedere gli eventi di massa, però, gli analisti dovranno fare attenzione ad un altro problema. Gli utenti dei social media non sono affatto un campione rappresentativo della società. Essi sono mediamente più istruiti, più ricchi e più giovani del resto della popolazione. Ancor più, i codici di comportamento sui social media sono diversi rispetto a quelli nelle interazioni in carne ed ossa, consentendo di solito una maggiore aggressività verbale. Spesso è proprio la rabbia ad indurre gli utenti a scrivere sui social media, sovrarappresentando l'indignazione. Prima di dedurre il sentimento di una popolazione in base a quanto gli internauti scrivono su Twitter, gli analisti, quindi, dovrebbero tenere a mente la relativa esiguità del campione sociale in analisi.

Come sfruttare i social media

Nonostante questi problemi, sarebbe imperdonabile per un'agenzia di intelligence non fare uso delle informazioni presenti sui social media. L'articolo analizza ora come sfruttare al meglio la SOCMINT da tre punti di vista: quello delle tecniche analitiche, della struttura organizzativa e del rapporto con i privati.

Problemi come il basso *signal-to-noise ratio* non sono affatto nuovi, ma vengono esasperati dalla quantità di informazioni disponibili sui social media. Nonostante siano problemi tradizionali, ancora non esiste una tecnica analitica in grado di risolverli[5] e occorre pertanto mitigarne l'impatto.

Il modo più semplice, ma anche il più efficace, è la triangolazione delle fonti. Se utilizzando solo la SOCMINT ci si trova di fronte ad un mare di informazioni di scarsa qualità, combinando la

SOCMINT con HUMINT e SIGINT, invece, si possono ricavare informazioni di grande valore. In quest'ottica, un caso di scuola è quello del simpatizzante per un gruppo terroristico, attivo sui social media e che progetti di compiere un attentato. Attraverso le sole tecniche di SOCMINT non sapremmo distinguere questo soggetto da tanti altri. Tuttavia, se grazie all'apporto di ulteriori fonti informative, come fonti umane o elettroniche, si riuscisse a qualificare questo potenziale terrorista come un soggetto di interesse, a quel punto si potrebbero sfruttare appieno tutte le potenzialità della SOCMINT.

Grazie alla network analysis, infatti, sarà possibile ricostruire la sua rete di contatti, identificando magari altre persone di interesse e componendo in maniera più chiara il quadro inerente la sua reale pericolosità. In base agli orari e ai luoghi da cui si collega, si potranno comprendere le sue abitudini. Ricostruendo la sua attività sui social media, si potrà ricostruire il suo percorso di radicalizzazione ideologica. Anche gli aspetti più personali potrebbero diventare di interesse. Un qualsiasi guaio con la legge, ad esempio l'uso di stupefacenti o di materiale pedopornografico, potrebbe diventare un'opportunità per raccogliere ulteriori informazioni. Conoscendo i suoi interessi e le sue vulnerabilità si potrà identificare meglio l'approccio migliore nel caso in cui si decida di reclutarlo.

Lungi dall'essere superati in importanza dalla SOCMINT, HUMINT e SIGINT diventano quindi la chiave di volta per sfruttare appieno proprio le potenzialità della SOCMINT stessa. È fuorviante dunque contrapporre un tipo di fonte ad un'altra. Al contrario, è la sinergia delle fonti che consente il loro pieno sfruttamento.

Parlare di sinergia delle fonti non è una vuota formula burocratica, ma ha importanti conseguenze anche sul piano organizzativo. Una comunità di intelligence in cui gli specialisti dei vari metodi di raccolta informativa lavorino fianco a fianco appare essere più efficiente di una comunità in cui gli stessi lavorino ciascuno in un'agenzia apposita. Da questo punto di vista, l'organizzazione italiana, con la divisione geografica tra AISE e AISI, sembrerebbe meglio strutturata rispetto all'intelligence americana o britannica, dove la divisione avviene invece per tipo di intelligence, con SIS e CIA che si occupano di HUMINT, laddove GCHQ e NSA si occupano di SIGINT. Non a caso, la recente riforma della CIA proposta da Brennan mira a creare centri interni alla CIA dove specialisti di varie discipline possano operare fianco a fianco.

Cosa può imparare l'intelligence dai privati nell'applicazione della SOCMINT?

La SOCMINT pone importanti questioni anche dal punto di vista della cooperazione con i privati, con cui la comunità d'intelligence contemporanea vive in un rapporto strettissimo e difficilmente scindibile. In questo contesto, il ruolo dei privati risulta fondamentale non solo per assicurare un miglior apporto informativo, soprattutto con riferimento a quelle realtà produttive in grado di penetrare e conoscere a fondo scenari sensibili e difficilmente accessibili, ma anche sotto il profilo del supporto tecnologico e del progresso metodologico.

Non è certamente un segreto che i privati abbiano imparato più in fretta del mondo pubblico a sfruttare al meglio le opportunità concesse dalle tecnologie e dalla rete Internet, incluse quelle derivanti dai social media. Da anni, infatti, il marketing, la comunicazione aziendale e successivamente anche il management, hanno imparato a basare le proprie scelte sull'analisi delle informazioni disponibili in Rete. Inizialmente ciò avveniva attraverso il ciclo classico di raccolta informativa, basato sull'accesso online alle informazioni pubbliche e a quelle presenti in banche

dati proprietarie, alla loro analisi e sintesi attraverso le migliori tecniche analitiche e alla successiva creazione di *report* di interesse focalizzati sul fruitore finale. Oggi, invece, le decisioni dei privati utilizzano sempre di più le metodologie afferenti all'area della SOCMINT.

I vantaggi derivanti dalla SOCMINT sono molteplici, sia per i privati, che per le agenzie d'intelligence. Primo, l'enorme massa di dati costantemente riversati *online* dagli utenti aumenta la quantità delle informazioni raccolte. Secondo, la possibilità di interazione e persino di influenza delle fonti aumenta anche la qualità di queste informazioni. Terzo, l'automazione di alcuni processi intermedi consente di comprimere enormemente il lasso di tempo tra la raccolta delle informazioni e la consegna del *report* nelle mani del decisore.

Oltre alla maggiore quantità, qualità e rapidità, la SOCMINT consente di ottenere altri vantaggi nell'individuazione, raccolta e gestione delle informazioni. Nonostante il problema del basso *signal-to-noise ratio*, la SOCMINT permette infatti di individuare e creare delle mappe informative più puntuali, facilmente accessibili, monitorabili e soprattutto aggiornate in tempo reale rispetto a quelle realizzate attraverso il ciclo classico di raccolta informativa. A tal fine, inoltre, possono venire in soccorso anche alcuni metodi analitici – mutuati proprio dal settore privato – tesi ad individuare i soggetti ed isolare le informazioni rilevanti, come, ad esempio, le tecniche di *computational social network analysis*[6] e di *buzz monitoring*[7]. La *computational social network analysis* utile principalmente a ricostruire e studiare le forme di influenza e i gradi di connessione delle reti sociali di utenti. La *buzz monitoring*, invece, volta a quantificare e qualificare le conversazioni online su uno specifico tema. Ci si potrà, così, concentrare più facilmente sull'identificazione diretta dei soggetti 'leader' – in termini informativi – per ciascun settore d'interesse, monitorandone azioni e conversazioni in Rete, piuttosto che dissipare tempo ed energie nell'individuare le informazioni necessarie all'interno di banche dati proprietarie o peggio ancora attraverso un'analisi di tutto ciò che è pubblico. A ciò, peraltro, si affianca anche la possibilità di attingere agevolmente da aree e settori di conoscenza limitrofi o connessi rispetto a quello principale oggetto d'attenzione, ampliando così le prospettive di analisi e quindi anche la sua qualità. Tutto ciò è vero, come detto in precedenza, soprattutto nel caso in cui la SOCMINT venga anche correttamente indirizzata e supportata, ad esempio, da attività di HUMINT e SIGINT.

Una volta mappati i canali informativi ed identificati i leader, sempre attraverso la SOCMINT si potrà anche interagire direttamente con questi soggetti e cercare di influenzarli – persino sollecitando il rilascio delle informazioni. Le informazioni raccolte potranno essere tracciate (istantaneamente e senza confini) e aggiornate in tempo reale. In sostanza, l'interazione garantita dalla SOCMINT e l'interoperabilità delle informazioni raccolte attraverso di essa permettono di far evolvere la mera raccolta informativa passiva in una vera e propria 'caccia' alle informazioni utili all'analista.

In conclusione, in un'epoca che sta vivendo il passaggio dalla semplice digitalizzazione di tutte le informazioni alla loro 'datizzazione'[8], ovvero alla raccolta, registrazione, analisi e riorganizzazione di tutte le informazioni che vengono già nativamente create in formato digitale (come, ad esempio, i dati, ma anche le parole, la posizione geografica, le interazioni tra soggetti, ecc.), la gestione dell'enorme mole di informazioni detta *Big Data* rappresenta sì un problema, ma anche un'irrinunciabile opportunità per l'intelligence. Con una struttura organizzativa che faciliti l'utilizzo sinergico delle fonti e utilizzando tecniche che consentano di individuare e sollecitare le fonti online

e di creare le relative mappe informative, la gestione della mole di dati esistenti sui social media sarà più semplice, più proficua e più lontana dal problematico modello della 'pesca a strascico'[9]. La sfida per le agenzie di intelligence è epocale, ma in una società democratica che ha giustamente a cuore la privacy dei propri cittadini non si può chiedere loro nulla di meno.

Note

1 Per una discussione delle questioni etiche sollevate dalla SOCMINT e per il tentativo di identificare dei criteri per valutarne la legittimità, si veda D. OMAND, J. BARTLETT, and C. MILLER, *Introducing social media intelligence (SOCMINT)*, in «Intelligence and National Security», Vol. 27, No. 6, 2012, pp. 801-823, specialmente pp. 816-822.

2 Per approfondire, si veda quanto scritto da due di noi su questo sito: S. MELE, *La cooperazione pubblico-privato nella cyber-security*, disponibile sul sito del Sistema di informazione per la sicurezza della Repubblica, 2014, http://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/la-cooperazione-pubblico-privato-nella-cyber-security.html (ultimo accesso: 2 febbraio 2016) e C. AMERICA, *Servizi di informazione e intelligence economica a sostegno della competizione industriale*, 2014 disponibile sul sito del Sistema di informazione per la sicurezza della Repubblica, http://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/intelligence-economica-a-supporto-della-competizione-industriale.html (ultimo accesso: 2 febbraio 2016).

3 Harman, Jane, *Disrupting the Intelligence Community*, in «Foreign Affairs», marzo/aprile 2015, https://www.foreignaffairs.com/articles/united-states/2015-03-01/disrupting-intelligence-community (ultimo accesso: 2 febbraio 2016).

4 Si veda J. ROVNER, *Intelligence in the Twitter Age*, in «International Journal of Intelligence and CounterIntelligence», Vol. 26, No. 2, 2013, pp. 260-271, specialmente pp. 263-265.

5 Tra le 55 tecniche analitiche strutturate discusse da Richards Heuer e Randolph Pherson in *Structured Analytic Techniques for Intelligence Analysis*, CQ Press, Washington DC 2015, 2nd Edition, nessuna è dedicata al problema del basso *signal-to-noise ratio*. Per una discussione del problema relativo alla SOCMINT, si veda, ad esempio, N. ANTONIUS - L. RICH, *Discovering collection and analysis techniques for social media to improve public safety*, in «The International Technology Management Review», Vol. 3, No. 1, 2013, pp. 42-53, specialmente p. 51: «an adaptive technology to solve the "high noise, low signal" problem remains elusive», disponibile sul sito dell'Atlantis Press http://www.atlantis-press.com/php/download_paper.php?id=6264, (ultimo accesso: 2 febbraio 2016).

6 Per un'applicazione, si veda, tra gli altri, E. STAI, V. KARYOTIS, S. PAPAVASSILIOU, *Analysis and control of information diffusion dictated by user interest in generalized networks*, in «Computational Social Networks», Vol. 2, No. 18, 2015, disponibile sul sito della Springer Open http://computationalsocialnetworks.springeropen.com/articles/10.1186/s40649-015-0025-4 (ultimo accesso: 2 febbraio 2016).

7 Per un'introduzione al tema, si veda P. A. GLOOR et al., *Web Science 2.0: Identifying Trends through Semantic Social Network Analysis*, Institute of Electrical and Electronics Engineers, Computational Science and Engineering, 2009, Volume 4, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5284145 (ultimo accesso: 2 febbraio 2016).

8 V. MAYER-SCHONBERGER, e K. CUKIER, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, Houghton Mifflin, 2013.

9 Per un esempio di quanto detto, si veda, tra gli altri, W. MAGDY, K. DARWISH, I. WEBER, *#FailedRevolutions: Using Twitter to Study the Antecedents of ISIS Support*, Cornell University, 2015, http://arxiv.org/abs/1503.02401 (ultimo accesso: 2 febbraio 2016).