

ISSN 2421-4442

S T S

ICUREZZA TERRORISMO SOCIETÀ

Security Terrorism Society

INTERNATIONAL JOURNAL - Italian Team for Security, Terroristic Issues & Managing Emergencies



SICUREZZA, TERRORISMO E SOCIETÀ

INTERNATIONAL JOURNAL
Italian Team for Security,
Terroristic Issues & Managing Emergencies

2

ISSUE 2/2015

Milano 2015

EDUCATT - UNIVERSITÀ CATTOLICA DEL SACRO CUORE

SICUREZZA, TERRORISMO E SOCIETÀ
INTERNATIONAL JOURNAL – Italian Team for Security, Terroristic Issues & Managing Emergencies

ISSUE I – 2/2015

Direttore Responsabile:

Matteo Vergani (Università Cattolica del Sacro Cuore – Milano e Global Terrorism Research Centre – Melbourne)

Co-Direttore e Direttore Scientifico:

Marco Lombardi (Università Cattolica del Sacro Cuore – Milano)

Comitato Scientifico:

Maria Alvanou (Lecturer at National Security School – Atene)
Cristian Barna (“Mihai Viteazul” National Intelligence Academy– Bucharest, Romania)
Claudio Bertolotti (senior strategic Analyst at CeMiSS, Military Centre for Strategic Studies–Roma)
Valerio de Divitiis (Expert on Security, Dedicated to Human Security – DEDIHS)
Chiara Fonio (Università Cattolica del Sacro Cuore – Milano)
Sajjan Gohel (London School of Economics – London)
Rovshan Ibrahimov (Azerbaijan Diplomatic Academy University – Baku, Azerbaijan)
Daniel Köhler (German Institute on Radicalization and De-radicalization Studies – Berlin)
Miroslav Mareš (Masaryk University – Brno, Czech Republic)
Vittorio Emanuele Parsi (Università Cattolica del Sacro Cuore – Milano)
Anita Perešin (University of Zagreb – Croatia)
Giovanni Pisapia (Senior Security Manager, BEGOC – Baku – Azerbaijan)
Iztok Prezelj (University of Ljubljana)
Eman Ragab (Al-Ahram Center for Political and Strategic Studies (ACPSS) – Cairo)
Riccardo Redaelli (Università Cattolica del Sacro Cuore – Milano)
Mark Sedgwick (University of Aarhus – Denmark)
Arturo Varvelli (Istituto per gli Studi di Politica Internazionale – ISPI – Milano)
Kamil Yilmaz (Independent Researcher – Turkish National Police)
Munir Zamir (Fida Management&C7 – London)
Sabina Zgaga (University of Maribor – Slovenia)
Ivo Veenkamp (Hedayah – Abu Dhabi)

Comitato Editoriale:

Gabriele Barni (Università Cattolica del Sacro Cuore – Milano)
Alessandro Burato (Università Cattolica del Sacro Cuore – Milano)
Alessia Ceresa (Università Cattolica del Sacro Cuore – Milano)
Barbara Lucini (Università Cattolica del Sacro Cuore – Milano)
Davide Scotti (Università Cattolica del Sacro Cuore – Milano)

© 2015

EDUCatt - Ente per il Diritto allo Studio Universitario dell'Università Cattolica

Largo Gemelli 1, 20123 Milano - tel. 02.7234.22.35 - fax 02.80.53.215

e-mail: editoriale.dsu@educatt.it (produzione); librario.dsu@educatt.it (distribuzione)

web: www.educatt.it/libri

Associato all'AIE – Associazione Italiana Editori

ISBN: 978-88-6780-958-5

copertina: progetto grafico Studio Editoriale EDUCatt

Table of contents

RESEARCH ARTICLES

- MATTEO VERGANI, ANA-MARIA BLIUC
The evolution of the ISIS' language: a quantitative analysis
of the language of the first year of Dabiq magazine..... 7
- CLAUDIO BERLOTTI, ANDREA BECCARO
Suicide Attacks: Strategy, from the Afghan War to Syraq
and Mediterranean region. A triple way to read the asymmetric threats 21

ANALYSES AND COMMENTARIES

- LARIS GAISER
Intelligence economica: una proposta per l'Italia 63
- GIOVANNI GIACALONE
Islamic extremism from the Balkans emerges in Italy 87

FOCUS: WEB INTELLIGENCE

- MARCO LOMBARDI, ALESSANDRO BURATO, MARCO MAIOLINO
Dalla SOCMINT alla Digital HumInt.
Ricomprendere l'uso dei Social nel ciclo di intelligence 95
- ALESSANDRO BURATO
SOCial Media INTelligence:
un nuovo spazio per la raccolta di informazioni rilevanti..... 109
- MAURO PASTORELLO
How cyberspace is used by terrorist organization:
possible threats to critical infrastructures?
The most recent activities of cyber counterterrorism 117

FOCUS: GRANDI EVENTI

GIOVANNI PISAPIA

A Case Study Analysis of the Implementation of GIS Technology for Safety and Security Planning during Major Sport Events.....	137
Executive Summary.....	157

Dalla SOCMINT alla Digital HumInt. Ricomprensione l'uso dei Social nel ciclo di intelligence

MARCO LOMBARDI, ALESSANDRO BURATO, MARCO MAIOLINO¹

Fin dalla loro comparsa come medium di interazione di massa nei primi anni del 2000, i social media sono rapidamente diventati una preziosa fonte di informazioni per ricercatori di tutti i campi. Le persone spendono sempre più tempo della loro vita su piattaforme come Facebook, Twitter, Instagram, ecc. Attraverso questi social media, il web è diventato uno spazio in cui gli utenti possono rappresentare loro stessi, interagire in diversi modi e produrre e consumare costantemente informazione.

Diversi sono gli aspetti che intervengono simultaneamente a rendere l'argomento degno di un approfondimento in termini di possibile utilizzo da parte dell'intelligence. Il primo e fondamentale elemento riguarda la moderna concezione delle identità reali e virtuali (Tosoni, 2004; Grimmelmann, 2006; Peachey e Childs, 2011), non da concepirsi come separate ed indipendenti ma, al contrario, come estremamente interdipendenti e capaci di influenzare relazioni, motivazioni e azioni individuali ugualmente nello spazio virtuale e in quello reale. Una relazione, questa, non ancora del tutto esplorata riguardo agli aspetti di ordine e sicurezza e che evidenzia importanti lacune in ambito legislativo². Inoltre, sebbene sia forte la necessità di rinnovare il sistema di intelligence (Tomes, 2015, 2003; US Defence, 2009), a seguito principalmente dai fallimenti avvenuti in Afganistan e Iraq (Flynn *et al.*, 2010), ancora si stenta a integrare nell'analisi delle informazioni provenienti dai social media, e in generale, dalle altre fonti di raccolta dati, le scienze sociali e più precisamente i processi umani. Tali processi si fondano sempre più su sistemi di relazione che si attuano anche nel web 2.0, e sono ormai un elemento fondamentale per sviluppare una efficace comprensione e prevenzione delle nuove minacce, costantemente in evoluzione.

¹ ITSTIME – Università Cattolica.

² Tali lacune si riferiscono a processi giudiziari avvenuti in Italia, Germania, Paesi Bassi ed altre realtà nazionali europee, a seguito dei quali estremisti islamici sono stati rilasciati perché i processi di radicalizzazione on-line, definite come mero simpatizzare, e le prove relative alle attività effettuate da questi ultimi nel cyber spazio non costituiscono offesa per le varie legislazioni nazionali in questione.

Questo cambio di approccio e prospettiva sulle modalità di utilizzo e interpretazione dei dati che vengono raccolti dai social è infatti necessario per adeguare concetti, pratiche di sicurezza e di difesa alle sfide poste dalla Guerra Ibrida, una guerra diffusa, pervasiva e delocalizzata che è la cifra della moderna generazione di conflitti che superano il classico e geograficamente definito ingaggio di eserciti rivali, integrando una estrema liquidità alla presenza di nuovi attori ed innovativi campi di battaglia: «*a sophisticated campaign that combine low-level conventional and special operations; offensive cyber and space actions; and psychological operations that use social and traditional media to influence popular perceptions and international opinions*» (Hunter e Pernik, 2015).

Da una prospettiva legata all'intelligence, i social media hanno quindi la potenzialità di essere altamente importanti: più le nostre vite si collegano alla rete, più le nostre identità reali e virtuali si fondono, più informazioni rilevanti vengono condivise e sono quindi rintracciabili per elaborare analisi che siano le più complete possibili.

La Social media intelligence, o SOCMINT come è stata definita (Omand *et al.*, 2012), è la più recente componente del ciclo di intelligence che si concentra sulla raccolta e l'analisi delle informazioni che vengono prodotte e scambiate attraverso i social media. A ogni modo, sebbene il potenziale della SOCMINT si riconosca, gli analisti e i professionisti di intelligence spesso criticano l'assenza di una strategia, di una dottrina o di pratiche assodate sull'utilizzo di questo strumento di analisi. Il cambiamento dinamico del panorama che caratterizza l'ambito legato ai social media rende infatti necessario un approccio flessibile, in grado di adattarsi sia ai cambiamenti tecnologici che alla cultura legata all'utilizzo degli stessi. È infatti condivisa la posizione secondo cui non esista un prototipo definito di utilizzo di questa disciplina che deve invece rivolgersi le seguenti domande: su quale piattaforma sta avendo luogo la conversazione? Qual è la natura dell'interazione? Qual è l'oggetto della ricerca? Domande che, attraverso le loro risposte, definiscono la natura strumentale della disciplina che non può prescindere da una visione più ampia, che coniughi il processo di analisi puntuale delle informazioni con una contestualizzazione sociologica attraverso un processo sintetico che abbiamo definito DIGITAL HUMINT, connubio fruttuoso tra la pratica della Humint (Human Intelligence), parte costituente a pieno titolo e sin dalla sua origine del ciclo di intelligence, e l'approccio legato alle nuove fonti social.

In questa nota si citeranno solo alcune delle peculiarità comuni ai due ambiti per sottolineare le motivazioni della scelta, e dall'utilità, di una visione olistica dei singoli strumenti in una nuova disciplina, la DIGITAL HUMINT appunto.

1. *Real world vs digital world?*

Esiste davvero una contrapposizione tra il mondo digitale e quello reale? Se così fosse, a ragione, gli strumenti della SOCMINT e della HUMINT andrebbero considerati come declinati, il primo per occuparsi del mondo digitale, con le sue regole e le sue particolarità, e il secondo per il vero lavoro di intelligence, quello che ha a che fare con le persone e quindi porta a pezzi di informazioni più “autorevoli” e più facilmente “processabili” attraverso canali ormai rodati da parte dei servizi di informazione.

Aspetti, definiamoli pure sociali, come la rappresentazione, la comunità e l’interazione sono caratteristici della vita reale comune di chiunque, anche se (ormai la letteratura a riguardo ne è convinta) definiscono anche tanto profondamente il comportamento on-line delle stesse persone che ugualmente sentono la necessità di creare una rappresentazione di sé nel mondo nel quale sono inseriti (reale o virtuale), di stringere legami con chi gli sta attorno (reali o virtuali), di interagire con coloro con i quali condivide esperienze (reali o virtuali).

1.1 **La rappresentazione: sei veramente chi vuoi far credere di essere?**

AmMESSO che nel mondo virtuale sia difficilmente raggiungibile una situazione di completo anonimato (Lapidot-Lefler e Barak, 2012), la rappresentazione di sé avviene in due momenti distinti: all’atto dell’apertura di un profilo (rappresentazione statica) e attraverso la costruzione progressiva dei contenuti che “popolano” il profilo stesso (rappresentazione dinamica). L’analisi delle due rappresentazioni, specie nelle loro discrepanze, è in grado di fornire elementi interessanti per l’elaborazione di un’analisi che tenga conto anche degli aspetti sociologici e non meramente dei dati aggregati circa le impostazioni dell’account o delle rilevazioni delle preferenze dell’utente.

Come di fatto dimostrato da alcune ricerche, esistono diversi ambiti in cui le inferenze deducibili dalla semplice analisi statistica non si dimostrano essere pienamente fondate: Kosinski, Stillwell e Graepelb (2013) hanno analizzato i like di Facebook di circa 58.000 volontari nel tentativo di analizzare la tipologia di informazioni che possono essere estratte da questa analisi e le inferenze che possono essere fatte dai dati raccolti. Raccogliendo una media di 170 like per ognuno dei partecipanti alla ricerca, lo studio ha dimostrato un’accuratezza nell’inferenza, a esempio, dell’etnia (Caucasico/Afroamericano) e del genere (Uomo/Donna) anche se ha evidenziato una carenza nella capacità di inferire sull’uso di alcool o droghe da parte degli utenti, comportamenti, tra l’altro, che fortemente risultano essere influenzati da una dimensione “sociale”.

Altro strumento altamente significativo per la rappresentazione di sé è l'uso e la scelta del linguaggio: come per il mondo reale, la condivisione anche online di un codice comunicativo è significativa dell'appartenenza a un determinato gruppo. Tutto questo è supportato dai risultati di diverse ricerche che hanno mostrato come l'utilizzo di determinate parole sia in grado di rivelare molto di più della personalità di un utente di quanto egli stesso possa immaginare (Summer *et al.*, 2012).

1.2 Le comunità: creare e ricreare il proprio gruppo

L'individuo è un "animale sociale" e per questo si caratterizza come all'affannosa ricerca di intessere legami con altri individui. La letteratura relativa alla definizione di "comunità" in ambito virtuale ancora dibatte su quali siano le discriminanti perché un gruppo si possa definire tale. Ai nostri scopi è sufficiente che sia riconosciuto che per esistere una comunità coloro che la formano devono interagire tra di loro secondo delle norme condivise, una cultura digitale comune o altre caratteristiche rilevanti.

È evidente che aspetti come le modalità di creazione delle comunità on-line, il loro sistema di relazioni e la loro tipologia possono essere diversi rispetto a quelli che definiscono comunità o gruppi tradizionali. L'analisi delle comunità virtuali, quando volta a comprendere le motivazioni di appartenenza dei singoli individui, non può prescindere da considerazioni che riguardino questi aspetti. Per esempio, è necessario precisare ed essere consapevoli che esistono social pensati appositamente per ricreare una specie di copia della comunità reale (Facebook) e altri che invece creano gruppi che non hanno nessuna, se non minima, trasposizione effettiva e vera nel mondo reale. È proprio lo studio di queste comunità virtuali, a volte fortemente coese e con un alto grado di identificazione, spirito di appartenenza e condivisione delle finalità tra i propri membri, uno degli aspetti più complessi da affrontare ma al contempo altamente significativo che deve essere ricompreso nell'analisi della SOCMINT (Benthall, 2012).

1.3 L'interazione

Se con il termine interazione si intende tutto ciò che permette agli utenti di entrare in contatto l'uno con l'altro, condividere informazioni o collegarsi in qualche modo, nel momento in cui le persone decidono di entrare in contatto con altri individui nel mondo offline, esistono limitate possibilità di scelta circa gli strumenti per farlo: chiamare l'altro, mandare una lettera, presentarsi, ecc. Nel mondo online, strumenti come i retweet, i like, i preferiti e le condivisioni sono stati adattati per facilitare un insieme complesso di metodi indiretti di interagire con un individuo.

Boyd, Goldern e Lotan (2010) hanno condotto una ricerca circa le motivazioni per cui gli utenti utilizzano questo strumento:

- amplificare o diffondere il messaggio al pubblico,
- intrattenere o informare un pubblico specifico,
- commentare un tweet ri-postandolo e aggiungendo nuovi contenuti,
- dimostrare la propria presenza come un ascoltatore,
- dimostrare pubblicamente il proprio consenso,
- convalidare il pensiero altrui,
- dimostrare amicizia e/o fedeltà richiamando l'attenzione, spesso anche chiedendo di ri-postare,
- conferire maggior visibilità o persone o contenuti poco visibili,
- aumentare il proprio numero di contatti da un utente più visibile.

Dal punto di vista del processo di intelligence, in riferimento all'analisi dei profili individuali risulta assai interessante il tema della dimostrazione di amicizia e/o fedeltà. Utenti che vogliono rendere pubblica l'influenza che altri hanno su di loro, che vogliono dimostrare la loro stima nei confronti di individui dei quali condividono opinioni, spesso ri-postano questi contenuti per dimostrare tutto ciò in maniera indiretta. Questo rapporto, che non prevede un contatto diretto, incoraggia gli utenti a utilizzare gli strumenti della condivisione o del retweet scervi dal sentimento sociale dell'imbarazzo: la condivisione, infatti, rappresenta un'opzione a basso-rischio per interagire con un altro utente, con il quale probabilmente altro tipo di interazione sarebbe stato impossibile.

Complici di questi comportamenti sono due teorie distinte: *l'observation effect* e il *disinhibition effect*. Il primo fenomeno, noto anche come il paradosso dell'osservatore, si verifica quando gli eventi in una determinata situazione che si vuole indagare risentono della presenza dell'osservatore. Gli utenti dei social network, nel momento in cui hanno la percezione di essere osservati, possono reagire cambiando il proprio comportamento online o nascondo informazioni interessanti ai fini dell'analisi (Heppner *et al.*, 2007). Il secondo invece, riguarda il cambiamento di comportamento che viene assunto online dagli utenti che, avendo percezione di anonimato e non dovendo interagire faccia-a-faccia con il destinatario della loro azione comunicativa, tendono ad interagire di più e ad assumere toni anche più accesi di quelli che verrebbero utilizzati in caso di comunicazione offline (Lapidot-Lefler and Barak, 2012).

2. Conclusione

Le considerazioni riportate nell'articolo sono solo alcune di quelle necessarie affinché lo strumento della SOCMINT, efficace in termini di metodologia per la raccolta di "pezzi di intelligence" dal mondo virtuale, possa essere

ricompreso in una disciplina più ampia in grado di contestualizzare meglio, sia in termini di efficacia che di comprensibilità, le sue potenzialità.

L'identificazione delle aree di interesse sulle quali focalizzare la propria indagine raggiunta grazie alla SOCMINT deve infatti arricchirsi della consapevolezza che non esiste una netta distinzione tra mondo reale e virtuale in termini di rappresentazione di sé e senso di appartenenza. Vanno dunque fuse la SOCMINT e la HUMINT favorendo la nascita della loro sintesi in una nuova disciplina: la DIGITAL HUMINT.

Riferimenti bibliografici

Benthall, S. (2012) "Weird Twitter" art experiment method notes and observations. Digifesto, [Online]. Disponibile su: <http://digifesto.com/2012/10/18/weird-twitter-art-experiment-method-notes-and-observations/> [verificato 30 Settembre 2015].

Boyd, D., Golder, S. e Lotan, G. (2010) Tweet, Tweet, Retweet: Conversational Aspects of Retweeting on Twitter. Proceedings of the 43rd Hawaii International Conference on System Science, January 6.

Flynn, M.T., Pottinger, M. and Batchelor P.D. (2010) Fixing Intel: a Blueprint for Making Intelligence Relevant in Afghanistan, Voices from the Field, Centre for a New American Security.

Grimmelmann, J. (2006) Virtual Borders: The Interdependence of Real and Virtual Worlds, Peer-Reviewed Journal on the Internet.

Heppner, P.P., Wampold, B. E. e Kivlighan, D.M. (2007) Research Design in Counselling, Belmont: Thomson Higher Education.

Hunter, E. and Pernik, P. (2015) The Challenges of Hybrid Warfare, International Centre for Defence and Security, Tallin.

Kosinski, M., Stillwell, D. e Graepel, T. (2013) Private Traits and attributes are predictable from digital records of human behavior. Proceedings of the National Academy of Sciences of the United States of America, 110(15).

Lapidot-Lefler, N. e Barak, A. (2012) Effects of anonymity, invisibility, and lack of eye-contact on toxic online disinhibition. Computers in Human Behaviour, 28(2).

Omand, D., Bartlett, J. e Miller, C. (2012) Introducing Social Media Intelligence (SOCMINT). Intelligence and National Security, 7(6), 801-823.

Peachey, A. and Childs, M. (2011) Reviewing Ourselves: Contemporary Concepts of Identity in Virtual Worlds, Springer 2011

Sumner, C., Byers, A., Boochever, R. e Park, G.J. (2012) Predicting Dark Triad Personality Traits from Twitter usage and a linguistic analysis of Tweets.

Proceedings of the IEEE 11th International Conference on Machine Learning and Applications ICMLA 2012.

Tomes, R.R. (2003), *Informing US National Security Transformation Discussions: an Argument for Balanced Intelligence, Surveillance and Reconnaissance*, *Defence Studies*, 3(2).

Tomes, R.R. (2015) *Toward a Smarter Military, Socio-Cultural Intelligence and National Security*, *The US Army War College Quarterly Parameters, Contemporary Strategy and Land-power*, 45(2).

Tosoni, S. (2004) *Identità Virtuali: Comunicazione mediata da computer e processi di costruzione dell'identità personale*, Franco Angeli, Milano.

US Defence Science Board Task Force (2009) *Understanding Human Dynamics*, Office of the Under Secretary of Defence for Acquisition, Technology and Logistic, Washington DC.

From SOCMINT to Digital Humint. Re-frame the use of social media within the Intelligence Cycle

Since their first appearance as medium of mass interaction, in the early 2000s, social media have rapidly become a precious source of information to researchers of different fields. People spends an increasing amount of their daily time on social platforms such as Facebook, Twitter, Instagram and so on. Through those social media, the web became a space within which users may represent themselves, interacting in different ways, and produce and consume information constantly.

Different are the aspects that simultaneously intervene to make the argument valuable to be deepened, in terms of possible use from the intelligence side. The first and fundamental element concerns the modern understanding of real and virtual identities (Tosoni, 2004; Grimmelmann, 2006; Peachey and Childs, 2011), which are not to be seen as separated and independent from each other but, quite the opposite, as extremely interdependent and able to influence relations, motivations and individual actions, equally, within the real and the virtual space.

This relation, that remains to be fully explored in relation to its security aspects, still presents important lacks in legislative terms³. Besides, although

³ These lacks refer to judicial processes brought about in Germany, Italy, the Netherlands and other national realities, that caused the release of Islamic extremists because the processes of radicalisation via web, defined as mere support, and the relative evidences gathered from their cyber activity, do not constitute any offence within the underlined legal frameworks

the need to renovate the intelligence system is strong (Tomes, 2015, 2003; US Defence 2009), mainly due to its failures in Afghanistan and Iraq (Flynn *et al.*, 2010), still there is a kind of reluctance to integrate social sciences and particularly Human Dynamics within the analysis of the information gathered through social media and, in general, from other sources of data collection. These dynamics are increasingly based on systems of interactions that are activated on the web 2.0, and are, nowadays, a crucial element to develop an effective comprehension and prevention of new and constantly evolving threats.

This change of approach and perspective on the use modes and data interpretation that get picked up from social media, is in fact necessary to adapt security and defence concepts and practices to the new challenges posed by Hybrid Warfare, a diffused warfare, pervasive and de-localised, that is the mark of the new generation of conflicts. They overcome the classic and geographically defined engagement of rival armies, integrating an extreme liquidity to the presence of new actors and innovative battlefield «*a sophisticated campaign that combine low-level conventional and special operations; offensive cyber and space actions; and psychological operations that use social and traditional media to influence popular perceptions and international opinions*» (Hunter e Pernik, 2015).

From the intelligence perspective, social media have then the potential to be highly important: the more our lives connect to the web, the more our real and virtual identities merge up, the more relevant information get shared and, so, the more they become traceable and available to elaborate as the most complete analysis as possible.

Social media intelligence (SOCMINT, Omand *et al.*, 2012), is the youngest component of the intelligence cycle, that is focused on the collection and analysis of information produced and exchanged through social media. However, despite SOCMINT value is recognised, analysts quite often criticise the lack of a strategy, a doctrine or best practices on the use of this specific instrument.

The dynamic change of the environment characterising the social media domain, makes necessary a flexible approach, that is able to adapt to technological changes and their utilisation culture as well. It is in fact shared the position according to which a defined prototype of the use of this discipline does not exist, it needs, instead, to be asked the following questions: Which is the platform supporting the conversation? Which is the nature of the interaction? What is the research object? Demands that, thanks to their answers, define the instrumental nature of the subject, that may not avoid a wider vision, integrating the process of developing a detailed analysis of the information gathered with a sociological framing, through a synthetic effort

that we define as DIGITAL HUMINT, fruitful union between the HUMINT practice, primary constituent, since its very origin, of the intelligence cycle and the approach connected to social media sources.

Within this note, some peculiarities related to both of the domains will be discussed, with the aim of underlining the choice's motivation, and the usefulness of adopting a holistic vision of formerly independent instruments within a new framework, DIGITAL HUMINT again.

1. *Real world vs Digital world?*

Does it truly exist a clash between digital and real world? If this is the case, reasonably, the SOCMINT and HUMINT tools should be considered as declined, the first to deal with the digital world, with its rules and specificities, and the second to the true intelligence business, the one that deals with people and hence leads to more authoritative pieces of information, more easily processable via known channels and information services.

Aspects, definable as social, such as self representation, community and interaction are classical of real life, common to everyone, even though (and the literature is sure about it) they also deeply define the online behaviour of the same people whom equally feel the necessity to create a self representation in the world the live in (real or virtual), to build up ties with who is around (real or virtual subjects) and to interact with the people sharing common experiences.

1.1 **The representation: Are you actually the person you want to make us believe to be?**

Given that in the virtual world the achievement of complete anonymity is pretty difficult (Lapidot-Lefler and Barak, 2012), the self representation comes in two different moments: when a profile is opened up (static representation) and through the progressive construction of the contents featuring that very profile (dynamic representation).

The analysis of the two representations, especially about their inner discrepancies, is able to provide interesting elements to the elaboration of an outlook that takes into account the psychological aspects as well, and not merely the aggregate data related to the account settings or the preferences manifested by the user.

As effectively demonstrated by some researches, there exist different domains where the deducible inferences, from the simple statistical analysis do not demonstrate to be fully reliable: Kosinski, Stillwell and Graepelb (2013)

analysed the Facebook likes of about 58.000 volunteers, attempting to understand the typology of information that may be extracted from that analysis and the inferences that may be done from the gathered data. Gathering an average of 170 like for each of the participants to the research, the study demonstrated an accuracy in the inference, for example, of the ethnicity (Afro/Caucasian), the gender (Man/Woman), even though denoting a weakness in inferencing over the abuse of alcohol or drugs from the users (behaviours that are strongly dependent on a social dimension).

Another highly significant instrument to self representation is the use and choice of the language: as for the real world, the also online sharing of a communication code is a valuable indicator of the belonging to a certain group. All this, is supported by the results of a number of researches that proved how the use of specific words is able to tell quite much about a user personality, surely a lot more than how much he may personally imagine (Summer *et al.*, 2012).

1.2 Communities: create and re-create our groups

Human beings are “social animal”, and because of that they continuously look for connections to other individuals. The literature concerning the definition of “virtual community” still argues on the kind of discriminants under which a group may define itself as such. To our purpose is sufficient to recognise that, in order, for the community, to exist, its members must interact to each other following shared norms, a common digital culture or other relevant features.

It results evident how aspects as the modalities of online community creation, their relations system and their typology may be different from the ones defining traditional groups or communities. The virtual communities analysis, when devoted to the understanding of the belonging of their single individuals, may not forget considerations related to those aspects. For example, it is necessary to specify and be conscious of the existence of social media that are thought precisely to re-create a copy of a certain real community (Facebook) and others, instead, that create groups having only a minimum degree of transposition into the real world. It is right the study of these virtual communities, sometimes strongly united and featured by a high level of identification, spirit of belonging and goals sharing between their members, one of the most complex element to be faced but, at the same time, extremely significant and that must be re-considered by the SOCMINT analysis (Benthall, 2012).

1.3 The interaction

If, with the term interaction it is intended everything allowing users to get in contact with each other, sharing information or connecting in some way, when people decide to get in contact with other individuals in the offline world, there exists limited possibilities of choice regarding the tools to do it: calling, mailing, self introduction and so on. In the online world, tools such as re-tweet, likes and shares have been adapted to facilitate a complex system of indirect methods to get in touch with the other.

Boyd, Goldern and Lotan (2010) conducted a study on the motivations behind the users adoption of those instruments:

- to amplify or diffuse the message to the public
- to entertain or inform a specific audience
- to comment a tweet, re-posting it and adding new contents
- to demonstrate the presence as listener
- to publicly demonstrate consensus
- to validate the other's reasoning
- to demonstrate fidelity and friendship re-calling the attention, often asking to re-post as well
- to give more visibility to people or contents that are hardly visible
- to increase the number of contacts from a more visible user

From the intelligence process point of view, referring to the analysis of individual profiles, it results to be very interesting the demonstration of friendship/fidelity theme. Users whom want to make the influence that others have on them public, whom want to demonstrate their respect to the individual of which they share contents, often re-post those contents to demonstrate their appreciation indirectly. This relationship, that does not foresee a direct contact, encourages users to use the sharing or re-tweet tools freed from the embarrassment sentiment: sharing, in fact, represents a low risk option to interact with another user, with whom another kind of interaction would have otherwise been impossible.

Two distinct theories are the drivers of such behaviours: *the observation effect* and *the disinhibition effect*. The first, also known as the observer paradox, materialise when the events of a given situation, that needs to be detected, suffer from the observer presence. Social media users, when they perceive to be observed, may react changing their behaviour online or hiding interesting information to the scope of the analysis (Heppner *et al.*, 2007). The second, instead, concerns the behavioural change assumed online by users that, having the anonymity perception and not having to interact face to face with the receiver of their communicative action, tend to interact more and more heartedly than if they would have faced the same situation in the offline world (Lapidot-Lefler and Barak, 2012).

2. Conclusion

The considerations reported within this article are only some of these necessary to allow the SOCMINT tool, already effective in terms of methodology and gathering of “intelligence pieces” from the virtual world, to be re-framed within a wider discipline better contextualising, both in terms of effectiveness and comprehensibility, its own potential.

The identification of the areas of interest over which to focus the research, reached thanks to SOCMINT, must be enriched with the consciousness regarding the fact that a neat distinction between real and virtual world, in terms of self representation and belonging, does not exist. SOCMINT and HUMINT need to be fused, facilitating the birth of their very synthesis: the discipline of DIGITAL HUMINT.

References

- Benthall, S. (2012) “Weird Twitter” art experiment method notes and observations. Digifesto, [Online]. Disponibile su: <http://digifesto.com/2012/10/18/weird-twitter-art-experiment-method-notes-and-observations/> [verificato 30 Settembre 2015].
- Boyd, D., Golder, S. e Lotan, G. (2010) Tweet, Tweet, Retweet: Conversational Aspects of Retweeting on Twitter. Proceedings of the 43rd Hawaii International Conference on System Science, January 6.
- Flynn, M.T., Pottinger, M. and Batchelor P.D. (2010) Fixing Intel: a Blueprint for Making Intelligence Relevant in Afghanistan, Voices from the Field, Centre for a New American Security.
- Grimmelmann, J. (2006) Virtual Borders: The Interdependence of Real and Virtual Worlds, Peer-Reviewed Journal on the Internet.
- Heppner, P.P., Wampold, B. E. e Kivlighan, D.M. (2007) Research Design in Counselling, Belmont: Thomson Higher Education.
- Hunter, E. and Pernik, P. (2015) The Challenges of Hybrid Warfare, International Centre for Defence and Security, Tallin.
- Kosinski, M., Stillwell, D. e Graepel, T. (2013) Private Traits and attributes are predictable from digital records of human behavior. Proceedings of the National Academy of Sciences of the United States of America, 110(15).
- Lapidot-Lefler, N. e Barak, A. (2012) Effects of anonymity, invisibility, and lack of eye-contact on toxic online disinhibition. Computers in Human Behaviour, 28(2).
- Omand, D., Bartlett, J. e Miller, C. (2012) Introducing Social Media Intelligence (SOCMINT). Intelligence and National Security, 7(6), 801-823.

Peachey, A. and Childs, M. (2011) *Reviewing Ourselves: Contemporary Concepts of Identity in Virtual Worlds*, Springer 2011

Sumner, C., Byers, A., Boochever, R. e Park, G.J. (2012) Predicting Dark Triad Personality Traits from Twitter usage and a linguistic analysis of Tweets. Proceedings of the IEEE 11th International Conference on Machine Learning and Applications ICMLA 2012.

Tomes, R.R. (2003), Informing US National Security Transformation Discussions: an Argument for Balanced Intelligence, Surveillance and Reconnaissance, *Defence Studies*, 3(2).

Tomes, R.R. (2015) Toward a Smarter Military, Socio-Cultural Intelligence and National Security, *The US Army War College Quarterly Parameters*, Contemporary Strategy and Land-power, 45(2).

Tosoni, S. (2004) *Identità Virtuali: Comunicazione mediata da computer e processi di costruzione dell'identità personale*, Franco Angeli, Milano.

US Defence Science Board Task Force (2009) *Understanding Human Dynamics*, Office of the Under Secretary of Defence for Acquisition, Technology and Logistic, Washington DC.

La Rivista semestrale *Sicurezza, Terrorismo e Società* intende la *Sicurezza* come una condizione che risulta dallo stabilizzarsi e dal mantenersi di misure proattive capaci di promuovere il benessere e la qualità della vita dei cittadini e la vitalità democratica delle istituzioni; affronta il fenomeno del *Terrorismo* come un processo complesso, di lungo periodo, che affonda le sue radici nelle dimensioni culturale, religiosa, politica ed economica che caratterizzano i sistemi sociali; propone alla *Società* – quella degli studiosi e degli operatori e quella ampia di cittadini e istituzioni – strumenti di comprensione, analisi e scenari di tali fenomeni e indirizzi di gestione delle crisi.

Sicurezza, Terrorismo e Società si avvale dei contributi di studiosi, policy maker, analisti, operatori della sicurezza e dei media interessati all'ambito della sicurezza, del terrorismo e del crisis management. Essa si rivolge a tutti coloro che operano in tali settori, volendo rappresentare un momento di confronto partecipativo e aperto al dibattito.

La rivista ospita contributi in più lingue, preferendo l'italiano e l'inglese, per ciascuno dei quali è pubblicato un Executive Summary in entrambe le lingue. La redazione sollecita particolarmente contributi interdisciplinari, commenti, analisi e ricerche attenti alle principali tendenze provenienti dal mondo delle pratiche.

Sicurezza, Terrorismo e Società è un semestrale che pubblica 2 numeri all'anno. Oltre ai due numeri programmati possono essere previsti e pubblicati numeri speciali.

EDUCatt - Ente per il Diritto allo Studio Universitario dell'Università Cattolica
Largo Gemelli 1, 20123 Milano - tel. 02.72342235 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione) - librario.dsu@educatt.it (distribuzione)
redazione: redazione@itstime.it
web: www.sicurezzaerrorismosocieta.it
ISBN: 978-88-6780-958-5



Euro 20,00