WORKING PAPER
JANUARY 2018

UNIVERSITÀ
DEGLI STUDI
FIRENZE

THE SOCIAL MEDIA INTELLIGENCE: COLLECTION AND ANALYSIS OF INFORMATION FROM CYBERSPACE

DOMENICO FRASCÀ

Center for Cyber Security and
International Relations Studies

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,
Internazionali e Imprenditoriali (CCSSII)
Università degli Studi di Firenze
Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Le dichiarazioni e le opinioni espresse nella presente relazione sono unicamente quelle dell'autore e non implicano l'approvazione da parte dell'Università di Firenze, del Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali o del Center for Cyber Security and International Relations Studies.

Center for Cyber Security and
International Relations Studies

THE SOCIAL MEDIA INTELLIGENCE: COLLECTION AND ANALYSIS OF INFORMATION FROM CYBERSPACE

Domenico Frascà

UNIVERSITÀ
DEGLI STUDI
FIRENZE

Working Paper

January 2018

ABOUT THE AUTHOR

Domenico Frascà is a freelancer who works in the sector of business, political and association consultancy. He is project manager of the Luigi Einaudi Foundation. He is currently attending the II level Master in Leadership and Strategic Analysis at the Institute of Aeronautical Military Sciences (ISMA). He graduated in "International Relations and European Studies", master's degree course, at the "Cesare Alfieri" School of Political Sciences in Florence. He attended the Postgraduate Course in "Intelligence and National Security" at the University of Florence in collaboration with the Department of Information for Security (DIS), also winning a scholarship for merit. He attended a training course on United Nations negotiation processes and techniques at “Consules” which ended with a simulation of UN diplomatic work in New York. He is a member of the Center for Cyber Security and International Relations Studies of the University of Florence. He attended the 2015 Summer School intensive course "Negotiations in humanitarian crises" at the Institute for International Political Studies (ISPI) in Milan. He is mainly interested in strategic studies, geopolitics and national security, but in general he has a passion for history and political science.

THE SOCIAL MEDIA INTELLIGENCE: COLLECTION AND ANALYSIS OF INFORMATION FROM CYBERSPACE

1.1 The Social Media Intelligence (SOCMINT)

Focusing on the opportunity to get knowledge from the enormous amount of data present in social media, a limited part of the doctrine specifically began to discuss social media intelligence (SOCMINT). SOCMINT, like any other intelligence activity, is universally aimed at filling a situation of lack of information and, therefore, favoring decision makers (Bonfanti, 2015).

Through the collection and analysis of data generated by attitudes and gestures that users manifest or perform in the virtual dimension of social media, SOCMINT allows its user, whoever it is, to grasp and understand facts and phenomena that originate and perform in this dimension. Moreover, SOCMINT can potentially contribute to provide a better understanding of events or phenomena that have already occurred, for which there is an interest in investigating the origin or causes that led to the triggering of that fact or phenomenon; indeed, a reconstruction ex post from the epiphenomenon to the phenomenon (Bonfanti, 2015). The most passionate supporters of SOCMINT, such as J. Harman, former member of the Intelligence Control Committee of the American House of Representatives and President of the Wilson Center for International Scholars, pushes on affirming that the value of intelligence gathered on social media will be greater than that collected using traditional methods such as Human Intelligence (HUMINT) (Mele, Faini, 2017). With one example, J. Harman goes on to say that, to monitor events in Ukraine, the CIA does not need a source within the Russian government, as the best reports are publicly accessible on social media (Harman, 2015).

Today we facilitate the task of those who want or should spy on us by publishing updates, in digital form, of our life minute by minute (Baker, 2010). This immense and inestimable amount of information, often unconsciously generated by us, is greedily preserved by the companies that provide us with the services - often essential - which, with an adequate mix of data at their disposal, can compose a puzzle of our social behavior and staff (Caligiuri, 2016).

Facebook, the most famous social media in the world, reconstructs in detail the activities and the network of relationships of more than a billion users, therefore people, meticulously marking out the way we communicate, even our preferences regarding books, places, films and much more (Caligiuri, 2016).

Understanding social media and their content is a great opportunity to contain, and respond to threats - coming from cybernetic space - which make public habits unsteadable every day. Social media becomes an important public space where you can tap into relevant news to monitor users with malicious intentions (Omand, Bartlett, Miller, 2012a).

In the coming years, on the terraqueous globe, physical identities will be less than virtual ones, moreover it is estimated that in 2020 the devices connected to the internet could be fifty billion, or four times the terrestrial population (Kissinger, 2015). From these observations we understand how the incessant collection of data and news, and their control, is important and becomes a sphere of interest where the thin border between civil and military becomes derisory (Cukier, Mayer-Schoenberger, 2013).

Thanks to the knowledge acquired by “enabling technologies” and their pervasiveness, data collection seems increasingly simplified by the coming of “machine-to-machine” systems, where it seems to take more and more field and autonomy smart objects compared to other commitments of human character (Martino, 2012). Nowadays social media are the most used tool for interpersonal communication (Teti, 2015), depicting an exceptional container of personal information constantly increased and nourished with information, which distinguish the life of every single user. As a result of this, it is evident that social media can represent a learning context capable of bestowing an in-depth knowledge of this *mare magnum* of information.

This *mare magnum* of information, if efficiently and promptly collected and analyzed, allows not only to understand and clarify the heterogeneous social cases, but also to foresee them (Ceron, Curini, Iacus, 2014). The “forecast” is one of the most attractive opportunities that the social media world can offer to those who want to exploit the data present in this frame of cyberspace in order to possess an “advantage”.

Cybernetic space is a substantial and indispensable dimension for the search for information (ie the social nature of intelligence), so much the better if it is open sources or legally and ethically available (Caligiuri, 2015).

With the pervasiveness of new media, the decadence of textual information is emerging, replaced by other channels (video, photos, audio) which require particular analysis and study techniques (Teti, 2015). A large part of the research of Open Source Intelligence is made up of Big Data, from which it is possible to obtain predictive information relevant to intelligence since, through the analysis of Big Data, the study of relations developed on social media or 'analysis of telephone conversations, allow the specific and detailed reconstruction of the network of personal relationships and above all the degree of intensity with which they interact (Caligiuri, 2017).

Faced with the complicated, multiform and turbulent international system, the Intelligence services is increasingly indispensable and fundamental; in front of the chaos and uncertainty that the international system generates, they are necessary to know how to distinguish, identify and discover every possible scenario (Gori, 2015).

The Anglo-Saxon doctrine has devoted much attention to SOCMINT, coining both the form and the content, defining the notion at the beginning: a practice aimed at deriving knowledge from the multiplicity and variety of data and metadata that are generated and / or shared by individuals through their participation in virtual and social platforms (Omand, Bartlett, Miller, 2012b). It is easy to assume that a large number of actors, for example, those working in the security and defense sector, in the public administration sector, in the health sector, more in general in the economic-productive sector, can be interested in using this form of intelligence.

The understanding and predictive skills that derive from such intelligence practice are functional to the possibility of making decisions in certain circumstances with the aim of achieving specific objectives and, when implemented, will produce more amplified effects in the real and material dimension rather than in the virtual dimension.

The SOCMINT, by its logical and philosophical nature, as well as other intelligence practices, is not absolutely true knowledge because there is always the possibility of a denial; knowledge conceived through the Intelligence method is never completely true as it cannot be considered conclusively demonstrated (Antiseri, Soi, 2013). Moreover, this is a practice with variable information quality, that is, dynamic.

1.1.1 *The dinamism of social media*

The dynamism is given by the fact that the information transmitted by the social media platforms may be subject to a modification of contents that contribute to redesign, little by little, the form and degree of validity of the information. The interaction between users can be perceived as the engine of informational realization since interaction is the identifying characteristic of social media.

From this interaction, therefore, a variegated raw data content is derived, that is conspicuous of constituent elements that can be particularly relevant for an intelligence analyst. The element that characterizes the information originated from social media consists in its dynamism. Unlike the information generated by the news open source, in most cases, those spread by social platforms have a modification of content in itinere contributing to redefine, step by step, the backbone and the degree of validity of information; indeed, the data or final data are defined during the search and collection of the news because, thanks to the concurrence of other content integrations that come into contact with it, the information extracted from the news will be mutable to the changing of intervening variables (Sperini).

1.1.2 *Execution of SOCMINT*

The mode of execution of SOCMINT always admits the search and data collection with subsequent processing and analysis; the latter, in most cases, is performed through the use of tools and processes generally known as social network analysis. These procedures are characterized by their peculiarity, that is they are carried out, almost entirely, in an automatic way (machine-to-machine), that is through the use of technologies, which allow a quick and sharp processing of information (Bonfanti , 2015).

Some of these techniques and technologies are diversified on the basis of software and applications operating on the "Application Programming Interface (API)" of social media, e.g. Facebook Graph API, Twitter Graph API, etc., and other applications together with additional means and algorithms oriented to collect information in a structured and coherent manner such as “scrapers”, “crawlers”, “spider” (Bartlett, Miller, 2013). Since the amount of social media data is so large, several computational approaches have been developed to automatically infer and extract “meaning” without the occurrence of a human analyst; the most significant approach is a variant of the Artificial Intelligence – “machine learning” - where machine learning allows a series of important applications, from the identification of clusters and anomalies in large data sets, to the extraction of information from the text (Omand, Bartelett, Miller, 2012b).

An especially relevant application is the analysis of feelings, in which an algorithm searches for certain qualities and properties in a text that considers statistically correlated with a certain emotion or a “feeling” and, once the human input has defined the feelings in question, the algorithm can, with varying degrees of specificity and precision, automatically classify huge volumes of data on the same basis (Omand, Bartelett, Miller, 2012b).

Paradoxically, more the impact of new technologies and the amount of data increases, the more the “human factor” of intelligence becomes essential and fundamental to contextualize them; since by analyzing disparate sources of news, the intelligence analyst should be able to use a method by which to transform news into knowledge, “using the method of attempt and error, proceeding by conjecture and refutation, hypothesis and criticism, ready to change strategy and opinion in the face of inaccuracies, feeding, through experience and education, an open mind to change” (Caligiuri); indeed, the scientific method is an essential tool in order to approach the understanding of the facts. In the field of intelligence research, it is therefore indispensable “to be scientific, not [...] in the sense of being carriers of an exact science, but as a method, that is, to consistently continue to question everything, continue to verify, above all be ready to change your mind” (Antiseri, Soi, 2015).

The oldest element of intelligence is back in vogue: the human element, oriented simultaneously to analysis and operation, with the need for the integration of “knowledge”, merging humanistic and scientific skills, thus returning to the indivisible concept of culture (Caligiuri).

Social network analysis (SNA) is an approach that harmonizes sociological and mathematical methods in order to describe the intensity and frequency of relationships between people or small groups and is addressed to the understanding of individuals who are strongly influenced by a series of ways behaviors marked by the social bonds that surround them (Omand, Bartlett, Miller, 2014). By defining the structural peculiarities of these social bonds, SNA attempts to explain and illustrate the behavior of the network in general and the behavior of those who use it on the basis of their position within it (Omand, Bartlett, Miller, 2014). Once collected the data can be used for dissimilar purposes, ranging from the estimate of how many individuals are engaged in a specific online activity to understand the flow of information, to the elaboration of more complex analysis systems (Sparrow, 1991).

The Social Network Analysis activities typically used on social media, according to Omand, Miller and Barlett are:

- To monitor the evolution of a content produced on a specific case or a specific place;
- To monitor the dissemination of a given information flow;
- Monitoring of information sharing between individuals;
- Understanding the complex structures created by the behavior of individuals who influence the information that other users receive, and the behaviors that these communities adopt.

Mainly the security authorities, they could use this potential to better understand public behavior, such as those that may present themselves in a crisis situation, for example the manifestations of panic when shortages of key products or services occur, or to understand “herding” phenomena.

It is believed that this type of SOCMINT is potentially useful and important for what concerns the fight against terrorism and more generally public security (Omand, Bartlett, Miller, 2014).

1.2 SOCMINT as an Intelligence discipline?

As described, SOCMINT aims to be a further discipline of Intelligence as much as HUMINT, SIGINT, IMINT etc. Instead, it seems more difficult and controversial to establish a firm position between the relationship between social media intelligence and intelligence from open sources, or OSINT (Bonfanti, 2015).

Part of the doctrine suggests considering SOCMINT as a branch of the OSINT, since they are publicly accessible information and can be legally acquired by request, purchase or observation (Schaurer, Florian, 2012).

The doctrinal approach just suggested is criticized and rejected by the promoters and supporters of SOCMINT, since social media intelligence does not easily fit into the category of open or secret intelligence, since it bases its existence not by the fact that it seeks information from open sources but rather from the existence of social media; it is in fact responsible for the collection and management of data, according to a different degree of accessibility, inserted by users on virtual platforms, such as social media (Bartlett, Miller, 2013). Some of these data may also be of the "closed" type, that is reachable, under certain conditions, by a few authorized parties; only this element would suffice to disprove the previous doctrinal approach and not to insert SOCMINT under the "hat" of Open Source Intelligence. Again, if in the case of the OSINT the news is tended to be given, in the social media the content is generated and evolves within them, thus not allowing, definitively, the "completeness" of the news except in specific time periods, this because of the possible intervening variables that can act to damage or enrich the news; this dynamism of social platforms helps to clarify the identity character of the SOCMINT category (Sperini). Although social media have different structural and operational characteristics, they are accumulated by the concept of dynamism of their contents that evolve over time and cybernetic space by implementing the information system and the importance of a potential information chain (Sperini).

It is essential to underline that, whatever the preferred doctrinal configuration, it is necessary to realize that SOCMINT is also considered part of the intelligence system, that is, its "product" is intended to interact, where possible, with other intelligence disciplines (Bonfanti, 2015); in this way the concept of all-source intelligence is taken up again, that is the kind of information that derives from the use of all the available sources, for example through the integration of information provided by confidential sources with those taken from open sources.

1.3 Prevention and control of threats to national interests

“Before going to attack in May 2015 a demonstration in Texas dedicated to the satirical cartoons of Muhammad, Elton Simpson announced his intent on Twitter, launching the hashtag #Texasattack. [...] Just before the attack, the FBI had sent an alert to the local authorities, but it does not seem that the message arrived in time to allow further protective measures to be taken” (Mele, Faini, America).

Many people talk openly under the spotlight of social media and, rather than hiding interests and sympathies for terrorist groups, they directly declare their connection and their plans for future attacks; Cases like Elton Simpson's become more and more common. Following an attack, at times we realize that in order to hinder and prevent it would be enough to monitor what these, alleged terrorist, publish on their social pages. Unfortunately, it is not enough to add “Al Qaeda” or “Islamic State” to friends on Facebook in order to get in touch with them to unveil and defeat these kinds of projects. Nevertheless, the intelligence that can be derived from exploiting the news on social media, becomes increasingly essential, with the aim of countering threats to the national interest (Mele, Faini, America,).

There are several subjects who in recent years use cyberspace for criminal purposes and, above all, for purposes related to the propaganda, support or fulfillment of international terrorist acts, more precisely, “individuals and, more or less organized groups exploit the potential of the Network to perform actions that vary from activities informative/misinformation and espionage, networking, propaganda, fundraising, proselytism and recruitment, training, up to the planning and coordination of boycott campaigns, predatory actions, acts of sabotage, psychological warfare and cyberterrorism” (Bonfanti, 2015).

Social media is already a “space” where criminals associate, communicate and plan to commit crimes; as early as 1999, almost all known terrorist groups had established a presence on the Internet (Von Behr, Reding, Edwards, Gribbon, 2013). The transition from traditional websites to online social networks, built around interactive forums, allows the sharing of varied communications, where leaders often publish stories and piloted discussions (Omand, Miller, Bartlett, 2014).

In most cases and increasingly, social media reach vulnerable and marginalized young people with difficulty in integrating into real society; this happens because, social media, turn out to be a means of communication where you can exclude unwanted people, and isolate yourself with other individuals, who have a vision of reality similar to their own, thus forming a network of people who "think about at the same way" (Bartelett, Miller, 2013). An obvious opportunity that SOCMINT offers to law enforcement authorities is: spontaneous help from citizens because, in their most direct form, platforms like Twitter or Facebook can act as a new channel of communication that allows users to share information, including videos and photos, in real time with the police, thus obtaining direct evidence against the criminals; the most common complaints sent to the police are those that belong to the sphere of hate interest: such as racism, anti-semitism, threats or incitement to violence (Omand, Miller, Bartlett, 2014).

CONCLUSIONS

SOCMINT, with its diverse use in different spheres of interest, has the capacity to produce the knowledge necessary to improve decision-making in a large number of public sector organizations, contributing and improving the information available to those who need to make sensitive decisions about public safety. According to Omand, Bartlett and Miller, this ability is divided into three different levels (Omand, Miller, Bartlett, 2014).

The first level is to help the authorities to establish situational awareness at the same time as carrying out particular events such as peaceful demonstrations or not. From the analysis of social media, we can identify essential facts of the world: when events occur, what is currently happening, where and who is involved.

The second, certainly very complex, is to construct the best causal explanation of the events that occurred as they were observed; then the why and the manner in which the activities in question were carried out, from a complex act of terrorism to the simple street crime. The second level of analysis, claims a very high degree of general understanding of the phenomenon in question and the terms with which the subjects in question usually express themselves. Given the appropriate explanations of the events and motivations for which the participants in the "fact" have joined, it will then be reasonable then, to look for a prediction on how the events will take place.

This third level of analysis provides for a more complex use of this form of intelligence, in order to respond to the inevitable interrogations of political and operational authorities regarding what and where the "fact" will take place. This ability to explain and forecast, is essential aimed to plan a peremptory response to threats to public safety, trying to shape the current situation through the use of different forms and scales of response by the authorities that address the issue. With the knowledge that can derive from SOCMINT it is possible to monitor in real time a rapidly evolving situation and the geographical granularity of the information, giving the possibility to alter the sensitivity and therefore the degree of the response, minimizing the risks of alienating the community or provoke an overly violent attitude of force in relation to the answer (Omand, Miller, Bartlett, 2014).

The usability of a legitimate, timely and resolving social media intelligence can contribute decisively to public security, especially SOCMINT acquires this role, when it is integrated and exploited together with other categories of intelligence, ie disciplines such as HIMINT, SIGINT, MASINT, IMINT etc.

Listening to social media using "Big Data" acquisition and analysis tools can help authorities identify emerging events, study networks and groups of individuals, discern public attitudes and improve situational awareness. The advantages of using SOCMINT are related to the wide range of information available on social networks and the speed with which they are accessible and obtainable.

SOCMINT has the potential to improve and compensate for decision-making ignorance and provide actionable intelligence, ie information with immediate operational impact that allows institutional users - government decision-makers, military commanders, police forces - to take instant initiatives in order to counter a threat deemed imminent. So SOCMINT is certainly an important part of the future of intelligence work; however, like all forms of intelligence, their use by the authorities can have consequences in the real world for individual citizens. Surely one of SOCMINT's strengths is the direct access, in a tactical situation, to the feelings and emotions of those involved in a given situation. In contrast, SOCMINT is weaker if information is not submitted to the collation system with other types of sources. For example, in crisis states or chaotic protest situations, care should be taken to ensure that monitored media exchanges truly reflect the overall view of the population or express the feeling of only those who "love" using social media. Another weakness of social media intelligence is the collection and analysis errors that can occur due to the high amount of news that the analyst is exposed to, namely the c.d. low signal-to-noise ratio, in addition to the fact that this information obtained, more often than not, is taken out of context.

The more the impact of new technologies and the amount of data increases, the more the “human factor” of intelligence becomes essential and fundamental in order to contextualize them; the most ancient element of intelligence is back in vogue, the human element is oriented simultaneously to analysis and operativity, with the necessity of the integration of “knowledge”, merging humanistic and scientific competences, thus returning to the indivisible concept of culture (Caligiuri). The future of SOCMINT is linked to the individual who inserts more and more elements of his life off-line in an online environment; Jamie Bartlett supports this last idea, stating that in 10-15 years each government department will have its own center of social media analysis (Liviu, Anamaria, Codruta, Nicolae, 2015).

According to Sir D. Omand, looking to the future, it will take: take into account the way in which technology can improve the monitoring of social platforms and the extraction of useful information, for example through the implementation of the analysis of computerized feelings that, with technological evolution, becomes more and more precise, de-structuring sentences, attributing roles, up to start a real human-machine dialogue. The third and fourth generation web services (web 3.0 and 4.0) focus on Artificial Intelligence, thanks to which automated systems can interact, in a completely autonomous way, with man. The Artificial Intelligence is useful to SOCMINT in order to mitigate the Data Deluge effect (literally “deluge of data”) since it is necessary to streamline the automatic computation of data more and more. “In other words, it is necessary to act directly on the raw data, operating on information independent from the databases” (Martino, 2015). According to all the doctrine dedicated to the topic, the area of activity in which SOCMINT will play an important role will be in crisis management to provide situational awareness to decision-makers, drawing news directly from those affected by the disaster or the crisis.

BIBLIOGRAPHY

ABBATE J., *Inventing the Internet*, MIT Press, Cambridge (Mass.), 1999.

ABDELHAQ V.H., SENGSTOK C., GERTZ M., "*Even Tweet: Online Localized Event Detection from Twitter*", in Proceedingg of the VLDB Endowment, Vol. 6 (12), 2013.

ANTISERI D., SOI A., *Intelligence e metodo scientifico*, Rubbettino Editore, Soveria Mannelli, 2013.

BAKER S., *Il potere segreto dei matematici. Chi sono i signori dei numeri che controllano il nostro comportamento: cosa compriamo, come votiamo, chi amiamo*, Mondadori, Milano, 2010.

BARTLETT J., MILLER C., "*The state of art: a literature review of social media intelligence capabilities for counter-terrorism*", in Demos Publishing, Novembre 2013.

BERNERS-LEE T., FRISCHETTI M., *Weaving the Web*, HarperCollins, San Fracisco, 1999; trad. it. *L'architettura del nuovo Web*, Feltrinelli, Milano, 2001.

BONFANTI M., "*Social media intelligence a salvaguardia dell'interesse nazionale Limiti e opportunità di una pratica da sviluppare*", in U. Gori e L. Martino (a cura di), *Intelligence e interesse nazionale*, Aracne editrice int.le S.r.l., Ariccia (RM), agosto 2015.

CALIGIURI M., *Cyber Intelligence. Tra libertà e sicurezza*, Donzelli Editore, Roma, 2016.

CALIGIURI M., "Cyber intelligence, la sfida dei data scientist", *il mondo dell'intelligence*, pubblicato nel sito del Sistema di informazione per la sicurezza della Repubblica all'indirizzo: http://www.sicurezzanazionale.gov.it. [consultato il 10/01/18]

CASTELLS M., *Galassia Internet*, Feltrinelli, Milano, Terza edizione aprile 2010.

CERON A., CURINI L., IACUS S.M., *Social Media e Sentiment Analysis. L'evoluzione dei fenomeni sociali attraverso la rete*, Springer-Verlag Italia, Milano, 2014.

CUKIER K., MAYER- SCHOENBERGER V., "*The Rise of Big Data*", in Foreign Affairs, Vol. 92, Number 3, May/June 2013.

DI CARLO A., PAOLONI A. (a cura di), *Libro Bianco sul Trattamento automatico della lingua*, Roma, 2004.

FARRELL H., "*The internet's Consequences for Politics*", Annual Review of Political Science, Vol. 15:35-52.

GORI U., "Intelligence e interesse nazionale", in U. GORI & L. MARTINO (a cura di), *Intelligence e interesse nazionale*, Aracne editrice int.le S.r.l., Ariccia (RM), agosto 2015.

GORI U. E GERMANI L.S. (a cura di), *Information Warfare 2010. Le nuove minacce provenienti dal cyberspazio alla sicurezza nazionale italiana*, Franco Angeli, Milano, 2011.

HARMAN J., "*Disrupting the Intelligence Community*", in Foreign Affairs, marzo/aprile, 2015, https://www.foreignaffairs.com . [consultato il 10/01/18]

HOWE J., *Crowdsourcing: Why the Power of the Crowd Is Driving the Future of Business*, Crown Publishin Group, New York, 2008.

JOHNSTON M.J. & JOHNSTON R., *Testing the Intelligence Cycle Through Systems Modelling and Simulation*, in R. JOHNSTON, Analitic Culture in the U.S. Intelligence Community. An Ethographic Study, Central Intelligence Agency, Washington, D.C., 2005.

KAPLAN A.M., HAENLEIN M., "*Users of the world, unite! The challenges and opportunities of Social Media*", in Business Horizons, Vol. 53, 2010.

KISSINGER H., *Ordine mondiale*, Mondadori, Milano, 2015.

KOZINETS R.V., *Netnography: DoingEtnographicReserch Oniline*, SAGE Publications Ltd, New York 2009; A. Fabbro, *Cos'è la Netnografia*, E-book, 2013.

KUEHL D.T., "*From Cyberspace to Cyber-power: Defining the problem*", in F.D. KRAMER, S. STARR, L.K. WENTZ (a cura di), *Cyberpower and National Security*, National Defence University Press, Washington (D.C.), 2009.

LE BON G., *Psicologia delle folle, un'analisi del comportamento delle masse*, TEA Editore, 2004.

LIBICKI M.C., *Cyberdeterrence and Cyberwarfare*, RAND, Santa Monica (CA), 2009.

LIVIU A., ANAMARIA C., CODRUTA R., NICOLAE M., *Social Media Intelligence: opportunities and limitations*, CES Working Papers – Volume VII, Issue 2A, 2015.

MARTINO L., *La Quinta Dimensione della Conflittualità. La rilevanza strategica del Cyberspace e i Rischi di Guerra Cibernetica*, CSSII – Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali, Università degli Studi di Firenze.

MARTINO L, FONI S., "Data Mining e Social Network Analysis: gli strumenti al servizio della cyber intelligence", in U. GORI, S. LISI (a cura di) Cyber Warfare 2014. *Armi cibernetiche sicurezza nazionale e difesa del business*, Cyber Warfare Conference, FrancoAngeli s.r.l., Milano, 2015.

MCCUE C., Data Mining and Predictive Analysis. Intelligence Gathering and Crime Analysis. Second Edition, Elsevier Inc., 2007.

MELE S., FAINI M., AMERICA C., *Social media intelligence e sicurezza nazionale. La raccolta informativa sui social media*, pubblicato nel sito del Sistema di informazione per la sicurezza della Repubblica all'indirizzo: www.sicurezzanazionale.gov.it . [consultato il 10/01/18]

OHMAE K., *Il continente invisibile: oltre la fine degli Stati-nazione. Quattro imperativi strategici nell'era della rete e della globalizzazione*, trad. it. Di F. Marchei, Fazi, Roma, 2001.

OMAND D., BARTLETT J. & MILLER C., "*Introducing Social media Intelligence (SOCMINT)*", in Intelligence and National Security, Vol. 27, 2012.

OMAND D., BARTLETT J. & MILLER C., *#Intelligence*, Demos Publishing, London 2012.

OMAND D., BARTLETT J. & MILLER C., "Towards the Discipline of Social Media Intelligence", in C. Hobbs, M. Moran, D. Salisbury (a cura di), *Open Source Intelligence in the Twenty-First Century New Approaches and Opportunities*, Palgrave Mecmillan, 2014.

PHYNTION M., *Understanding the Intelligence Cycle*, Rutledge, New York, 2013.

RAMACCI F., SPANGHER G. (a cura di), *Codice Penale e Procedura Penale e Leggi Complementari*, Giuffrè Editore, Milano, 2014.

RAMPINI F., *Rete padrona. Amazon, Apple, Google & co. Il volto oscuro della rivoluzione digitale*. Feltrinelli, Milano 2014.

ROVNER J., “in the Twitter Age”, in *International Journal of Intelligence and CounterIntelligence*, Vol. 26, No 2, 2013, pp. 260-271.

SCHAURER, FLORIAN, *Social Media Intelligence (SOCMINT) – Same song, new melody?*, Open Source Intelligence, 2012, disponibile sul sito: http://osintblog.org/?p=1462 . [consultato il 10/01/18]

SCHMIDT E., COHEN J., *La nuova era digitale. La sfida del futuro per cittadini, imprese e nazioni*, Rizzoli Etas, Milano 2013.

SPARROW M., “Network Vulnerabilities and Strategic Intelligence in Law Enforcement”, in *International Journal of Intelligence and Counter Intelligence*, Vol. 5, No. 3, 1991.

SPERINI A., “*Implementazione del ciclo dell’intelligence tramite l’utilizzo della social media intelligence (SOCMINT)*”, Centro Militare di Studi Strategici (CEMISS).

STEFIK M. (a cura di), *The Internet Age: Social Technical, and Legal Challenger for a Networked World*, MIT Press, Cambridge (Mass.), 1996.

STERLING B., *Giro di vite contro gli hacker. Legge e disordine sulla frontiera elettronica*, trad. it di M. Tavosanis, Mondadori, Milano, 2004.

TETI A., *Open Source Intelligence & Cyberspace. La nuova frontiera della conoscenza*, Rubbettino Editore, Soveria Mannelli, 2015.

TETI A., “*Open source intelligence. L’attività di raccolta di informazioni attraverso fonti di pubblico accesso può aiutare la sicurezza*”, Il Sole24Ore, 13 settembre 2015, disponibile su http://nova.ilsole24ore.com/frontiere/open-source-intelligence/. [consultato il 10/01/18]

TOFFLER A., *Lo choc del futuro*, traduzione di Bruno Oddera, Sperling & Kupfer, Milano, 1988, ed. Orig. *Future Shock*, Bantam Books, New York, 1970.

VINCENT S.W., VICKERY G., *Partecipative web: User-Created Content*, OCSE, 2007.

VITALI F., “La geopolitica economica dei dati e il futuro del dominio. Dal controllo alla previsione. Il potere tra social media e manipolazione dell’azione sociale”, in *Nomos & Khaos. Rapporto Nomisma 2011-2012 sulle prospettive economico strategiche*, Osservatorio Scenari Strategici e di Sicurezza, Nomisma Spa, A.G.R.A., Roma, 2012.

VON BEHR I., REDING A., EDWARDS C., GRIBBON L., *Radicalisation, in the Digital Era: The use of the internet in 15 cases of terrorism and extremism*, RAND, Santa Monica, CA, 2013.

WHEATON V.K.J., RICHEY M.K., "*The Potential of SocialNetwork Analysis in the Intelligence*", in E-International Relations, 2014.

ZELIN A.Y., *The State of Global Jihad Online*, New America Foundation, febbraio 2013, http://www.newamerica.net/publications/policy/the_state_of_global_jihad_online#_edn . [consultato il 10/01/18]

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,
Internazionali e Imprenditoriali (CCSSII)
Università degli Studi di Firenze
Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Center for Cyber Security and
International Relations Studies