SOCIAL MEDIA INTELLIGENCE: OPPORTUNITIES AND LIMITATIONS

Adrian Liviu IVAN[*]
Claudia Anamaria IOV[**]
Raluca Codruta LUTAI[***]
Marius Nicolae GRAD[****]

Abstract: *An important part of the reform of the intelligence community is felt in the opening linked with the widening spectrum of methods and spaces which can be used to collect and analyse dates and information. One of these methods that produce large mutations in the system is connected to the world of social media which proves to be a huge source of information. Social Media Intelligence (SOCMINT), the newest member of the family INT's, is undoubtedly a separate domain, a practice rooted in the work of the intelligence community. This paper proposes a general characterization of the most important aspects of Social Media Intelligence, a brand new way for the intelligence community to collect and analyse information for national security purposes (but not only) in the context of the current global challenges. Moreover, the work is focused in identifying the further limitations and opportunities of this practice in the upcoming decade.*

Keywords: OSINT; social media; threats; intelligence; privacy
JEL Classifications: L820

In a world of complex interdependencies, globalised, dominated by technological advances, information and especially one who has the information it has the power. An important vector of the globalization process, the Internet, has conquered the world and has secured the role of the main generator of information in nearly all areas, producing true metamorphosis in everyday life. When we talk about information and when information is more than abundant, a change in approach is more than necessary for the intelligence community.

An important part of the reform that the intelligence community feels is linked to the fact that the spectrum of methods and places that can be used to collect and analyse intelligence is widening. The main mutation is connected to the rethinking of open source data and the progress of social media which are a huge source of information of any nature that is available for the intelligence community, but not only.

Social media gives us the ability to develop an avatar as close as possible to our true person through whom we can express our desires, arguments, and expose our main visions and important events in our lives. This leads to the development of new forms of communication with major implications for the intelligence community.

[*] Professor PhD, Babes Bolyai University, Cluj Napoca, Romania, e-mail: adrian_ivan2007@yahoo.com
[**] Teaching Expert, PhD, Babes Bolyai University, Cluj Napoca, Romania, e-mail: claudyayov@yahoo.com
[***] PhD Student, Babes Bolyai University, Cluj Napoca, Romania, e-mail: raluca_lutai@yahoo.com
[****] PhD Student, Babes Bolyai University, Cluj Napoca, Romania, e-mail: marius_grad@yahoo.com

When the society is developing new forms of communication, such as social media, public institutions, including the intelligence community must be responsible enough to react and adapt to the new trends. Based on these aspects, in the following we propose to characterise in general the most important aspects of Social Media Intelligence (SOCMINT), a method to collect and analyse intelligence that concerns national security purposes (but not only) by exploiting the social media environment, focusing on the advantages and disadvantages of this form of intelligence.

SOCMINT is an original, complex and interdisciplinary concept and quite recent to enjoy of a clear and generally accepted definition by all professionals in the field.

Social Media Intelligence (SOCMINT) represents, in the view of most experts, the process of identification, validation, collection and analysing data and information from social media using intrusive and non-intrusive methods, with the aim of developing products for national security (Norton-Taylor, 2015). Like any other form of intelligence SOCMINTs purpose is to be able to reduce the "unknown" that comes within any decision making equation.

Using SOCMINT as part of the business intelligence community brings many opportunities and challenges translated by a number of advantages and disadvantages arising from the nature of this INT.

Operating on the principle of legality and proportionality, by using SOCMINT', intelligence communities are able to monitor communities in proximity and capable to influence policy-makers and the beneficiaries of the intelligence process by choosing the optimal decision.

Through SOCMINT, the intelligence community can determine some behavioural patterns that can apply for certain groups or certain individuals or can know better and in detail certain groups. In times of crisis, SOCMINT is a source of real time information and an important element in their management. Also in this direction, SOCMINT can be used for intelligence to create more resilience regarding events or issues that may contribute to the disruption of the safety and secure environment, can predict and monitor the processes of radicalisation and violent behaviour, can contribute to the understanding of phenomena and is able to predict future trends.

Through instant updates offered by social networks, SOCMINT manages to be a form of real-time intelligence. Intelligence analysts are able to collect real-time information related to ongoing events, either ordinary or state of crisis events. Technology now allows each person holding a smartphone to become a journalist and an information provider. The London Riots form 2011 and the Arab Spring are edifying in this direction. These events have demonstrated the ability of social media to gather information in real time to facilitate and prioritise actions that are to be taken in order to

manage crisis. These events have demonstrated the ability of social media to gather information in real time and to facilitate and prioritise actions that are to be taken in crisis management.

Another advantage of Social Media Intelligence is that it uses and provides a large amount of data and information that can be accessed, stored or disseminated relatively easy (Omand *et al.*, 2012, p. 34). This advantage can be easily turned into a disadvantage while the abundance of information may put the analyst on difficulty. Often, the analysts may find themselves unable to transform large quantities of information from social media into useful and quality products for national security.

As products obtained through Open Source Intelligence the products obtain through SOCMINT involves relatively low costs. Unlike other forms of intelligence, like HUMINT, intelligence collected from social media is not life threatening for the officer, but can cause problems related to freedom and fundamental rights, matters related to privacy issues or other individual freedoms. Most of the data and information collected by SOCMINT are recent. This advantage can be easily deconstructed by the surprising dynamics of the online environment and the speed of information flow that goes through this space.

The enormous possibilities offered by social media brings many advantages, as the ability of the analyst to achieve a multi-source analysis which will be useful both in the collection and verification of information. Data and information that intelligence communities get to collect through SOCMINT can represent the starting point for planning other intelligence cycles that are involving other forms of information gathering.

In addition to these advantages, using Social Media Intelligence brings a number of disadvantages and challenges. The large amount of information provided by online sources can lead to serious over-loading and sampling errors that can affect the entire intelligence cycle. Given that a typical day activity on a social network like Facebook website translates into 4 billion data and information spread and 250 million new photos, to an analyst or an intelligence officer, a certain data or piece of information becomes a needle in a huge haystack. This situation was clearly stated by a British official that once said that this situation "is like searching the British Library for a page in a book without an index to refer to" (Omand *et al.*, 2012, p.25). All this great amount of information can produce major errors. Not only is it hard to get to the information you seek, but it is particularly important not to get lost along the way. If the officer gets lost in the sea of information he can formulate an erroneous position, flawed by other information that is not conclusive to the situation.

Beyond all this, the greatest challenge that requires the use of Social Media Intelligence is linked to matters of confidentiality and consent and the identification of the boundary between what is public and what is private. Given that the postmodern man disclosure of personal information is an

important part of his life, establishing a line of demarcation is a difficult thing to achieve. According to a study made by the Global Institute, 30 billion personal information is spread each month on Facebook (Omand *et al.*, 2012, p. 27). This information can be used by intelligence communities or third parties like companies of terrorist groups. In these conditions, the concept of privacy in the online environment has been metamorphosed.

SOCMINT big problem occurs when someone enters in the private space of others, when the intelligence officer uses intrusive methods to collect data and information. Therefore, it is more than important for the legislation to be adapted to such contexts. Currently, no state has succeeded in formulating the legal framework covering and resolving these issues and this can be because SOCMINT is a recent concept and a recent process. Coming from the desire to resolve this inefficiency, David Omand and his team made a series of six principles to be taken into account when it comes to intrusive SOCMINT[1].

The first principle is that an analyst that collects information must have a solid and a legitimate reason for resorting to intrusive actions that violate some privacy issues. The most powerful reasons that can be raised are: the national security interest and the prevention of phenomena that are infringing upon national security grounds involving the preservation of public order and safety. A second principle (2) is linked to integrity plea: each taken action must be justified in each stage of the cycle of intelligence. (3) The reasons for resorting to such methods must meet the principle of proportionality and necessity. That means that the damage caused by intrusion shall not exceed the damage caused by the threat. The intrusion must always be minimal and efficient. Principle four (4) discusses the establishment of a legitimate authority that can validate ethical and responsible any activity that disturbs the individual's privacy and confidentiality of online sphere. (5) The use of this form of intelligence must be the last resort and (6) the result of this intrusive process has to be largely positive. (Omand and Bartlet, 2012, pp. 44-48).

Errors that may arise from misuse of intrusive SOCMINT may endanger the safety and security of individuals and cause great damage to the image of the intelligence services, which will have to explain to the increasingly concerned about their online privacy[2], public opinion andthe violation of individual rights and freedoms. Even if Mark Zuckerberg, the Facebook creator once appreciated that *privacy is no longer a social norm* (Omand *et al.*, 2012, p. 19), the intelligence services should use

[1] In terms of classification, literature records two major forms of Social Media Intelligence: a. Open the SOCMINT, SOCMINT obtained through non-intrusive means and methods and b. Surveillance SOCMINT, SOCMINT obtained by the means and methods that are intrusive and governed by a legal framework.
[2] We refer here to recent scandals related to the leaking information produced by Edward Snowen and NSA issue that troubled the American intelligence community and increased reluctance of American public opinionm and not only.

social media information in understanding the distinction between public and private space, in accordance with individual rights and freedoms and the principles of proportionality and necessity.

In this context, it is necessary to create a legal and ethical framework that can manage and clarify every aspect of using information that comes from social media.

Conclusions

Theorised by Sir David Omand, immediately after the London Riots from 2011, SOCMINT or Social Media Intelligence is a process where by identifying, collecting, corroborating data and information form social media, the analyst can produce relevant intelligence for national security.

SOCMINT is both an opportunity and a challenge for the intelligence community that needs to manage information in the context of increasingly intense expression of the individual in the online environment.

The advantages of using SOCMINT are related to the low cost of the operation, large range of available information, and the speed with which they can be accessed and collected. SOCMINT is not life threatening but may endanger the integrity and confidence of the intelligence services when we are talking about intrusive forms of collection and analysis.

On the one hand, the postmodern individual is more open to expose personal data online, but on the other hand, is extremely concerned about the degree of privacy and confidentiality that we offer online. It is, along with the errors that may occur due to too high quantity of information that the analyst is exposed, the biggest disadvantage of SOCMINT. This disadvantage can be eliminated by establishing principles and a legal framework that clearly regulate activities that concerns aspects of privacy and confidentiality.

Intelligence communities need to adapt to the way people create and share information, and in this context, social media provides the opportunity and the challenge to be one step ahead of the problem. Intelligence communities need to understand the benefits of the information provided by this INT and to learn and use it at its true value.

The future of SOCMINT is linked to the individual who mainly put more and more elements of his offline life in an online environment. Jamie Bartlett (Leavey, 2013) supports this last idea, saying that in 10-15 years every government department will have its own social media analysis centre.

Acknowledgements

This work was possible due to the financial support of the Sectorial Operational Program for Human Resources Development 2007-2013, co-financed by the European Social Fund, under the project number POSDRU/159/1.5/S/140863 with the title „Competitive European researchers in the fields of socio-economics and humanities. Multiregional research net (CCPE)".

References

Leavey, J. (2013) *Social media and public policy. What is the evidence?, September 2013,* available at http://www.alliance4usefulevidence.org/assets/Social-Media-and-Public-Policy.pdf (accessed on 30.05.2014).

Norton-Taylor, R. (2012), "Former spy chief calls for laws on online snooping", The Guardian, 24th of April, available at http://www.theguardian.com/technology/2012/apr/24/former-spy-chief-laws-snooping. (accessed on 30.05.2014).

Omand, D and Bartlet, J. (2012), "A balance between security and privacy online must be struck", in *DEMOS.*

Omand, D., Bartlet, J. and Miller, C. (2012), "Introducing Social Media Intelligence (SOCMINT)" in *Intelligence and National Security*, Vol.27. No. 6, December.