THE EMERGENCE OF SOCIAL MEDIA INTELLIGENCE

Rareş-Adrian RAICU[*]

MOTTO:
"There are three kinds of intelligence: one kind understands things for itself, the other appreciates what others can understand, the third understands neither for itself nor through others. This first kind is excellent, the second good, and the third kind useless."
(Niccolo Machiavelli)

Abstract

In a world of constant change and with an environment of transnational security which varies depending on the fluctuations of international reality, intelligence is undergoing a series of mutations focused on a new typology of vulnerabilities, risks and threats to national, regional and international security. At the beginning of the millennium, the stages of globalization leave a prominent mark on society, as well as accelerate developments of information technology and science. All these are meant to facilitate the transition from the industrial age to the informational era and then to the knowledge society. In this context, asymmetric threats have diversified, both in number and intensity. Recent developments in technology and the shift from industrial society to the information society facilitated the dissemination means of these threats. Intelligence has been forced to adjust to the new requirements of the security environment and to develop new ways and methods to counter modern threats and risks.

Keywords: social media intelligence, modern threats and risks, informational era, knowledge society.

Introduction

In a world of constant change and with an environment of transnational security which varies depending on the fluctuations of international reality, intelligence is undergoing a series of mutations focused on a new typology of vulnerabilities, risks and threats to national, regional and international security. At the beginning of the millennium, the

[*] Romanian Intelligence Service.

stages of globalization leave a prominent mark on society, as well as accelerate developments of information technology and science. All these meant to facilitate the transition from the industrial age to the informational era and then to the knowledge society. «*The expansion of the virtual world led to the emergence of a new dimension of state power, "the digital power", with long term effects on strategic knowledge and on the state actions both national and international speaking. Also, the individual has acquired new tools, through access to databases and networks, tools that can influence directly the exercise of power, domestically or internationally. The recurrence of "Facebook" and "Twitter" revolutions form Europe to Middle East demonstrates the impact of these virtual instruments on the political regions, an impact that was unimaginable less than a decade ago. Evolving forms of "digital power" will represent, equally, development opportunities, but also vulnerabilities and security challenges, and their management will be determined by the ability to access, detect and use information*» (Maior, 2011, p. 2).

In this context, asymmetric threats have diversified, both in number and intensity. Developments in technology and the shift from industrial society to information society facilitated the increase in the dissemination means of these threats, intelligence being forced to adjust to the new requirements of the security environment and to develop new ways and methods to counter modern threats and risks.

The interpenetration and coexistence of some elements belonging to the informational era with the layer of the new knowledge society creates the current world context, at the beginning of the XXIst century. In this context, one can speak about a permanent necessity to adapt the specific intelligence activity to the new types of challenges, risks and emerging threats of the knowledge society and of those related to the informational era, characterized by dynamism and unpredictability. Today, information technologies are developing at a rapid rate, being disseminated faster and often not being used for creating a favorable security climate. The expansion of asymmetric threats, mentioned above, materialized in the form of terrorist or extremist groups or, more recently, as modern cyber threat uses all the benefits that the informational society can offer. Thereby, if until now one could speak, for example about a conventional terrorist spread rapidly by globalization and which could be materialized by exploiting national and international security breaches especially in the physical space, today one can speak about terrorism adapted to the new challenges of the informational era and especially to those knowledge societies that are fully exploiting the virtual opportunities.

Therefore, intelligence should be conceptualized and directed to a collection of data and information from all available sources, whether clandestine or public. The opening of intelligence and security services to the

civilian sector and the exponential growth of OSINT usage, without neglecting the HUMINT (Lesidrenska & Bancheva, 2014, p. 151) element and the other INT's, be it the MASINT, SIGINT, IMINT or even the specific means and methods of intelligence can guarantee intelligence services success in preventing and countering risks and threats to the knowledge society.

As mentioned earlier, the emergence of informational and communicational technologies also attracted, apart from opportunities, a number of vulnerabilities that by materialization and manifestation could seriously damage the international security climate. However, the rapid evolution of the phenomenon of social media and the current societal trend towards interaction and communication, due to the existence of online facilities has led some groups to act, not only in the tangible reality but also in the virtual sphere. So, through their assumed missions, namely to prevent and combat the risks and threats, on the one hand, and to promote and preserve national values, on the other hand, it was incumbent on the intelligence services to direct their activity also to this space, which had not been considered relevant until 9/11. This was a milestone start in understanding the effects of the virtual world on reality.

The starting point of the need to approach the phenomenon of social media is actually the summer of 2011, specifically on August 6. In London, significant street violence emerged with a powerful social impact. The population's grievances began with the shooting of Mark Duggan, a black Tottenham resident, in north London, by a police officer trying to arrest him. Although the reason for his arrest was not made public, many assumed that it was part of an operation of the Metropolitan Police, called *Trident*, which was investigating illegal possession of weapons and their use in drug trafficking or crimes by black minority in England. In the following days, social discontent spread throughout London taking various forms, mostly demonstrations against Great Britain's police structures. Further, as in the case of most demonstrations or protests, social discontent (Le Bon, 2012) transformed in vandalism and theft (Philips, Frost, Singleton, 2012, p. 1).

After Mark Duggan's assassination by the British police, a series of assumptions about his death began to spread in the black community, generating greater tensions that escalated quickly. If initially one could speak about a protest of a group of 200 people who asked for explanations about the man's death, soon things became complicated. Speculations about Duggan's death diversified. In this regard, there were a series of speculations that he was killed intentionally by the policeman who arrested him and that he was shot in the chest after being handcuffed. Another speculation regarded that he would have told his friends 15 minutes before his death that he was surrounded by police, but he was safe (Lewis, 7 august 2011). The uncertainty

about Mark Duggan's death was what actually created discontent among the protesters. Thus, they were accusing the Metropolitan Police that no shootout had occurred, that the man did not have a gun in his possession, and that his murder was against the law. Police reports would have indicated that he was carrying a gun, which was acquired even before being arrested from Kevin Hutchinson-Foster. The interrogations and the trials of the latter could not demonstrate and prove the charge. On January 8th, 2014 a verdict was reached that the death of Mark Duggan had not represented a violation of the law (*Mark Duggan inquest and reaction*, BBC News).

As has been noted, the protests began amid these uncertainties and based on the English black community's dissatisfaction. If, at first they spoke about a peaceful protest on the night of August 7th, 2011, the protests degenerated and created violence and tension. So, some questions appeared related to the speed of transformation of a peaceful protest, low as location and number of participants, into violent and widespread demonstrations. Initially the causes of protest's degeneration have been identified in the way the events were presented in the local press and TV stations with national coverage. *On the one hand everything was blamed on local media, and on the other hand on the UK's television.* However what customized the violence in London was the massive promotion of the social media phenomenon.

In this regard, on the social network Facebook, protesters began to create various groups, under different names (*Justice For Mark Duggan and Those Killed by Police*, *Justice for Mark Duggan aka Starrish Mark.Sho! Sho*, *R.I.P Mark Duggan* or *Justice for Mark Duggan*), online communities that expanded rapidly after the beginning of the protests. Some of them even reached 34.841 members (*Pagina oficială de facebook R.I.P. Mark Duggan*). Although more such groups appeared, all turned their attention to the same kind of content. Group managers asked supporters to take to the streets and to demand justice for Mark Duggan. Examples of postings on this (user Shannon Loch: *Screw Police Brutality* or user Milad Gh.: *Hey guys come on…I waiting for YOU! Are YOU with me?*) used generally more biased language, often accompanied by obscene words against the police or against what happened. Most posts on the Facebook social network aimed mainly, besides blaming what happened especially on London Police. These gathered a large number of supporters who were willing to take to the streets and participate in protests as seen in Milad Gh's post.

After more than three and a half years since Mark Duggan's death and since the bloody riots from England, these pages have not completed their activity and their managers continue posting messages against police and seeking solidarity for those killed by police officers *(The Police are the biggest Mafia, but only in this case in a uniform. Fact! BirminghamStrong Justice 4 ALL*

Justice For Mark Duggan aka Starrish Mark.Sho!Sho Stephen Lawrence Charitable Trust Campaign for Justice for Smiley Culture). Moreover, they frequently express their dissatisfaction with the events that happened. During the trial of Kevin Hutchinson-Foster, they asked people again to go out in the streets and support Mark Duggan's cause (*Judgement Day 2013! Let's make it big! Look on the post below for more info. Let's do this 1 time! March 15 at 1:00pm* or *Who coming Birmingham today for demo? Admin Tommy D, Plan B*). The offensive force of the online community in supporting and defending Mark Duggan could be observed on Facebook. Some persons were informal virtual leaders, had a specific coded language, and even promoted multimedia content to instigate and attract as many protesters taking part in violence. Thus, it was easy for them to find about the place and time of the violence from social media.

In addition to using the Facebook app, protesters resorted to exploiting the social media platform Twitter and to making their voices heard in support of Mark Duggan's cause. Through tweets, users of this network managed to quickly spread information, taking advantage of the idea of Internet SMS and all its benefits. Thus, through short messages, they quickly changed dates, particularly about the time and place of the protests and also messages requesting the arrival of a large number of protesters. An example of this can be the user's tweet @carboia, stating *Spoke to them. They're on their way. Be with you soon*, referring to the reunion of all protesters.

Differently from messages of calling supporters and protesters, Twitter's was also used, in the case of the riots that took place in London, as a vehicle of social media propaganda. In the days between 6th and 11th of August a series of rumors about the social dissatisfaction of the community and the forms that their protests took spread as Twitter posts. Tweets of users who claimed that protesters attacked London Zoo and managed to release the animals emerged. So @Twiggy_Garcia, a Twitter user which had 5.178 supporters, was the first that spread the rumors on the platform that protesters entered the zoo and freed all animals. This information appeared also with Twitter hashtag #LondonRiots. At 2 am on August 7th, the user @Deadfreaks spread some information that the riots escalated, and the protesters even managed to enter the fast-food chain restaurants McDonald's and cook their own food, rumor that appears with hashtag #Tottenham. In the same hashtag, @DeclanJMN provided some information which referred to the fact that a 16-year-old girl would have been beaten by London's police, which would have fueled even more the tensions and social discontent. Things went much further, and @andzadio posts within hashtags #LondonRiots, #Londonriot and #Prayforlondon disseminated images with the London Eye in flames, and the tweet was quickly assumed and easily spread, tightening the

state of uncertainty and tension among population. Another example of this, is that @jazz_kaur spreads, using #Londonriots and #birminghamriots, a rumor according to which the protesters are leading to Birmingham Children's Hospital (*The Guardian*, December 7, 2011).

However, all the rumors promoted by the aforementioned users through Twitter proved to be false, and ultimately denied even by the London police. All this information had clearly meant to create panic and tension among the population, who did not know exactly what was happening. Protesters used all these rumors to be able to promote their violent actions and gain image before the rest of the community, thus spreading chaos and, worst, tension.

Therefore, available information from Facebook and rumors spread through Twitter proved a possible tension that could extend across UK. Within days, things degenerated in social media. From simple posts related to the death of Mark Duggan and from the desire to avenge his killing, posts that showed violent intentions or massive community organization to express their intentions clearly and complaints against police emerged. Thus everything basically turned into a street riot, built out of violence, theft and conflicts that resulted in casualties.

After the dispelling of tensions and the calming down of both the protesters and their adversity to police and the calming down of the street riots, the Metropolitan Police reported that it was taken by surprise by the emergence of the social media phenomenon and they did not presume that carrying out intelligence in this virtual space, with everything that it implies, from collection and verification to analysis and integration, could have helped officers prevent and counteract the violent actions of protest. Thus, the need and the opportunity to create an office to collect and confirm the information available publicly in social networks, within intelligence departments, emerged.

Intelligence after London 2011. The emergence of a new discipline of gathering intelligence – SOCMINT

The events that took place in 2011 in London were the starting point in terms of the emergence of social media intelligence. Nevertheless, this concept appears quite late in the terminology of secret services, if we are to take into account the massive promotion of phenomena on the social networks, such as the Twitter Revolution in Moldova in 2009 or the Arab Spring from 2010. But the scientific literature accepts the riots in London as the starting point in the analysis and use of what means social media intelligence or SOCMINT, because the events were a lesson learned for the Metropolitan Police, being the first to realize the need of collecting

information also from this space. The Twitter Revolution in Moldova and the Arab Spring were seen as an important influence, as they were organized by extensive movements aimed at overthrowing the regimes in power, especially the communist ones, whose intelligence institutions had not considered or had only condemned and blamed social media involvement in the events that took place in 2009 and 2010, without taking into consideration the exploitation of all available information in social media.

Thus, overcome by the novelty and the speed with which information spread through social networks, departments specialized in gathering information from UK's Metropolitan Police were forced to take in their area of competence this virtual space too, assuming the mission to prevent and counteract threats from the online environment. Although at first many looked at that with skepticism, disregarding the new discipline of collecting intelligence, it began to play an important role amid the emergence of the informational era and knowledge society.

The head of London's Police Open Sources Department, Umut Ertugrul, declared that for OSINT he leads "*social media behaves like CCTV in terrestrial space*" (*Financial Review*), referring to the system of street surveillance cameras, available in England. According to Wired UK website, Scotland Yard would have recognized the existence of a team to monitor social networks and related posts that refer to political tensions. The team would be composed of 17 officers and would be named SOCMINT, having the mission to monitor Facebook, Twitter, YouTube and other social media services. This achieved 24 hours a day, 7 days a week continuity, stating also that this team of officers develop new means and methods to improve the intelligence activity. As a component unit of the Metropolitan Police, the team has jurisdiction in all districts of Great Britain and Wales (Wright, June 26, 2013).

Although through online media were circulated these information, tacitly recognized even by the OSINT director within London Police, Urmut Ertogral, there are still misunderstandings and uncertainties about what social media intelligence is or why it is necessary to approach SOCMINT among intelligence services.

Therefore, since the discipline is characterized by novelty, there still is no clear terminology of the phenomenon, but a series of works are starting, on the one hand, to tackle the issue directly, while on the other hand, other works study the related phenomenon. On this line, in the work Introducing Social Media Intelligence, considered the cornerstone of the approach SOCMINT, Sir David Omand outlines the new discipline as "*the existence of some capabilities through which authorities access data communication and access with warrant, when necessary, the communications content from the Internet, in this case social media*" (Sir Omand, Bartlett şi Miller, 2012, p. 802). He also claims that

the use of SOCMINT capabilities can contribute in a decisive way to ensuring public safety by identifying criminal activities, providing an early warning of the existence of tensions or public threat, or by creating a operational warnings when events evolve quickly (Sir Omand, Bartlett & Miller, 2012a, p. 9). Sir David Omand, together with his team, established what collecting intelligence from social networks means, which essentially can be summarized in gathering information available from the communication realized online via social media, also offering some examples of areas to ensure safety, be it national or international, as well as ways that SOCMINT can contribute directly to achieving this.

Other attempts to define what constitutes social media intelligence refer to "*collecting information from open sources by surveillance specialists in online socializing sites, chats, websites and Internet*" (*Use of Internet for Terrorist Purposes*, 2012, p. 68) or particularizes what SOCMINT means, as a subsequent area of collecting information from open sources, based on the idea that social media is an intelligence branch of OSINT, but has a specific action domain, in this case social networks (SOCMINT, October 26, 2012). Therefore it may be considered a new discipline of intelligence is emerging, still at an early stage of development and introduction to the work of the intelligence services. However, it is observed and materialized, even if for the moment, under the form of lessons learned, the opportunities that social media intelligence could provide with its implementation in the agenda of business information, opportunities that are not negligible, thanks to the contributions that they could make to ensure security.

Social Media Intelligence – opportunities for intelligence services

The lessons learned after the 2011 London riots lead to the necessity of introducing the concept of social media intelligence, as a new gathering intelligence discipline, among the classic ones like HUMINT or TECHINT, being at the same time a modern tool of harvesting intelligence, like CYBERINT. Research carried out regarding the London events and how the intelligence spread throughout the social media platforms revealed the fact that an analysis, realized in the spirit of the book and at a very specific moment in time, of the events released with the help of social media, would have been, in the end, a good early threat detection factor for Metropolitan Police, which, by using this tool, could have early combat and prevent the London riots and could prevent the swarm of conflict.

Therefore, taking into account all the things mentioned above, the perfect context for introducing SOCMINT on the working agenda of intelligence services was created, this new and young INT proving a series of opportunities of collecting primary data regarding a specific domain, such as

riots or social unrest, and after that it would contribute to guaranteeing of the security climate within the capitalization of an analysis realized by the analysts of intelligence services.

Speaking about the opportunities brought out by using social media intelligence, it is said that the added value offered to the intelligence activity consists of the easing of the work of secret services through the simplification of collecting data about periods of time, locations of unfolding of events or individuals participating to this events. Apart from all of that mentioned above, there are some key concepts which make the object of studying the opportunities of social media intelligence.

Therefore, speaking about the opportunities brought out by the phenomenon of social media intelligence, the need to understand the utility of the *crowd sourcing* concept appears. James Surowiecki, a well-known journalist from *The New Yorker*, speaks about the intelligence of crowds and, at the same time, about gathering intelligence from crowds. His theories are associated with the theory of Gustave Le Bon regarding the idea of crowd. Subsequently, he argues that the idea that a few individuals who approach a specific domain or issue will bring out a better solution for solving it, rather than this problem would be solved by a person or two. In his book, *Wisdom of Crowds*, he explains the concept of crowd sourcing, emphasizing an essential aspect, that when we talk about intelligence of crowds, we don't speak only about brains put together, but decentralization. So, more individuals, among an extensive collectivity, will approach a specific issue and each person will have a key solution to it. Therefore, according to the theory, the idea that, in the end, a specific person will bring the best solution needed to solve the issue is promoted (Surowiecki, 2005). This phenomenon can be observed among the social media platforms. At the very beginning it was established that users disseminate content and information on a social media page. For instance, in the particular case of London riots, each Twitter user posted own beliefs regarding the events. In this context, we can speak about crowd sourcing from social media platforms, because the Metropolitan Police had the chance to analyze all these tweets (gathering intelligence), to check them for validation (verification), to analyze in order to establish action directions (analysis) and, in the end, to choose the best way of action, all of the above being based on intelligence gathered from social media platforms, in order to prevent or counter the riots. By these means, the utility and the necessity of crowd sourcing activity can be proven, all these being pictured on the key core of intelligence activity, the intelligence cycle.

Another dimension of this phenomenon, in term of opportunity of SOCMINT for intelligence service, is generated by Sir David Omand, who is the promoter of the idea that speaking about crowd sourcing, from the

institutional point of view, we can speak about a better information flow between citizens and governmental institutions, especially when there are critical situations. He starts his research from the idea that persons who assist at the birth of a specific event can become journalists for a minute, having the chance to post on social media intelligence from the field, intelligence which can be subsequently used by intelligence officers. Through the facilities offered by social media, but especially throughout the possibility to disseminate multimedia content, these journalists can post photos or movies from the field, which can be used by law enforcement institutions in order to start new operations. By connecting the concept of crowd sourcing with the concept of wisdom of crowds, regarding the intelligence services` activity, a platform, was established called Ushahidi, where individuals can post intelligence, no matter of its nature, such as information regarding the Haiti earthquake or traffic jams from Washington (Sir Omand, Bartlett şi Miller, 2012, p. 805). Thus, with small steps, the basic levels of a new technology which can provide citizens with the chance to contribute actively to the security climate are established.

Another opportunity of the emerging social media may consist in the research and the insight of social network analysis. The study of the social media platforms could help the secret services understand certain emerging phenomena within WEB 2.0. This could reveal some essential facts, like violence indicators, Islamic terrorists' ways of promoting self-radicalization or limits and indicators of criminality brought by the social networks. Thus, this thing can contribute to the understanding of the possibilities of forming and changing certain ideas and for investigating the link between social media and technology, between an off-line status and an on-line (Sir Omand, Bartlett şi Miller, 2012, p. 805) one, for having a guarantee of a built-in knowledge of both the phenomena and their initiators.

Besides the above mentioned things, the opportunities provided by SOCMINT also include the concept of real-time operational intelligence of the activities developed in the virtual space of the social networks. The analysis of Twitter statistics revealed that there are postings both before and after the manifestation of a phenomenon. Therefore, the evaluation of the social media platform traffic, could facilitate the identification of emerging phenomena, a process carried out much easier as compared to the application of the traditional investigative techniques for the same purpose.

For instance, if the geolocation of the events promoted in the social media could be determined, then the intelligence analysts could obtain evolution maps for the possible new physical locations of a protest, revolt and, why not, of a criminal act (Sir Omand, Bartlett şi Miller, 2012, p. 805).

Regarding information gathering via the activities developed and promoted within the social networks, one could speak about knowing the people and groups developing such activities. Terrorist or extremist groups frequently create pages on Facebook or Twitter in order to promote their ideology, their messages, and their own values. Thus, intelligence officers are given insight into these groups, achieving a better understanding of their mentality and action modalities. In this sense, one could study the level of social discontent existing within the group, of the state of tension of its members or of the main motives that animate the users' activity.

SOCMINT can be also used by intelligence services to identify criminal, extremist or terrorist intentions through large scale monitoring operations of the social networks run by specialized technical officers who have the possibility to survey the activity of the groups and people known as developing actions which could pose a threat to national security (Sir Omand, Bartlett și Miller, 2012, p. 806).

However, it is not only the terrorist or extremist groups that organize themselves through social media in order to enlist new members. After the emerging social networks phenomenon, intelligence services have also begun a vigorous campaign of recruitment through this space. These campaigns have two directions.

On the one hand, one could speak about promoting security institutions and their transparency together with their call for personnel, following the model of private companies which by help of marketing campaigns promote their image and look for personnel. On the other hand, there is a particular aspect regarding the intelligence service, that is, recruiting new intelligence agents and appealing to the collaboration of resourceful people from the medium of interest. It follows then that, by combining a classical INT- HUMINT with a modern INT, that is SOCMINT, the intelligence platform is prepared to ensure security.

In this sense, for instance, the British Intelligence Services (MI6 and SIS) used a Facebook application to recruit their personnel, to fill out questionnaires and to attract people coming from different social media.

CIA has also created a Facebook page for recruitment only, Mark Zuckerberg's network being accused by different media that it would represent a means of the Central Intelligence Agency's activity due to the fact that the American service has invested large sums of money in the technology of social media surveillance. In this context, "the recruiting mode as well as the agency's coordination method and specific means of the intelligence activity observe the same conspiratorial rules, having the great advantage of a better conspiracy and a larger operational level"(Ciupercă, Ciupercă, Niță & Stoica, 2010, pp. 124-125) as all is done remotely, without exposing the intelligence

officers, as they operate behind a computer" (Ciupercă, Ciupercă, Niţă, Stoica, 2010, pp. 126-127). Under these circumstances, the intelligence services can operate in social media, under conspiratorial profiles, simulating real life cover either to establish connections with future agents or to get in the relational background of those targeted who, in their turn, due the anonymous character of the social networks could be more open to cooperating with intelligence services. At the same time, through these platforms, the intelligence officers could verify persons' alibi by comparing the stories they provide "to their activity within the social networks"(Ciupercă, Ciupercă, Niţă, Stoica, 2010, pp. 126-127).

However, if a future recruitment of possible sources or agents is commendable, this time in a real, tangible space, when the people in question are known as being active on social networks, the intelligence officers can collect primary data on them, by following some standard criteria, available, for instance on Facebook, thus obtaining the agent's or the source's profiling.

In this sense, a first step in the learning process can be the profile picture or pictures as well as other pictures posted on the user's page. If the intelligence officer has only the name of the person (or his username) listed in a relational circle of suspects, without having the possibility, at that given moment, of collecting other significant data and if other information previously recommended him for selection and recruiting, then the said officer can proceed with the verification of this person on Facebook.

If one or several profiles corresponding to the name obtained are found, the officer can identify the respective person by comparing data recorded in the population register with those found on Facebook, as to confirm the correspondence between the real name or the username and the Facebook profile. In this sense, one can compare the date of birth recorded in the population register with the date of birth of the profile, thus facilitating the above mentioned correspondence and the full identification of the checked person. Consequently, the intelligence officer can access the user's profile picture or pictures which results in identifying and knowing that person. Besides the physical aspects, the officer can gather information through posted pictures, about the user's relational circle, having, in this way, the possibility of watching both the way in which this person spends his leisure time and the people surrounding him; through this possibility he can identify the hobbies and even the vulnerabilities that he may use later. All this helps the officer in becoming acquainted with that person before the real meeting, as he has learned some details that he can use during their discussions concerning recruiting.

A further step in the fulfillment of the person's profile meant to be recruited, made by the intelligence officer is to survey the personal data

posted by the checked person on his personal page. In this respect, another helpful thing for the intelligence officer who has to determine that person's profile, is the exposure of personal data, data that some users choose to make public in their account.

These are data concerning date and place of birth, education, coursework in progress, employment, marital status, residence, relatives and other contact data (sometimes even email or phone number). There are also two subsections within this section, which allow the user to include an additional description about himself and to add favorite quotes from various writers. The above mentioned data help the intelligence officer to establish those significant details regarding the education level, family, income and also to determine the psychosocial and behavioral traits of the person involved, which following an attentive analysis, he can use to establish a psychological profile of that person.

The friends and the connections the user made on his personal page can constitute the next essential aspect which the intelligence officer is to take into account in order to establish the checked person's profile. Thus, the officer who builds the profiling through the analysis of the user's friendship relationships and of his other contacts from the social media, completes his knowledge on the relational circle of the person chosen for recruitment.

A careful observation of the people added on the user's account and the analysis of the close relationship they have with certain people can lead to understanding of a particular relational background and to establishing of its specific features by identifying the social status of the person, the social milieu he frequents as well as his most comfortable surroundings. Therefore, important data can be obtained concerning the motivation for recruitment or the creation of a favorable recruitment context.

Check-in option, together with location services offer a great opportunity to the person who analyzes the chosen user's profile. He can observe in real time where the chosen person is, at a given moment, if this person utilizes check-in function while being in a certain place. In this way, the officer knows precisely where the person is situated, following GPS coordinates given on Facebook and also the names of public or private locations available in check-in function. Consequently, if the person posts something, the approximate posting location can be determined so that the officer in charge could check the presence of the said person in a certain neighborhood, district, and region.

In this sense, the intelligence officers can appeal to this profiling method by means of social media, to obtain, through the analysis of a few key elements of the Facebook network, primary data concerning the future candidates for recruitment, which when corroborated and verified by

comparing them with other information collected from different sources, can give an overall picture on the recruitment of the new information sources, on their quality as well as on the psychological features which led to the start of the recruiting process.

If, at the information operations level of the intelligence activity one could speak about obtaining a profile based on primary data, gathered via social networks, about the candidates for recruitment, then, within the technical side of this activity – as it was stated that even in this area the information collecting activity develops observing the same rules, means, methods, and principles –, social media is backed up by opportunities such as social network analysis software, easy- to -use by the intelligence services analysts.

In this context, a series of programs have been created whose utility in social network analysis is given by the easy way they produce graphical representations as a cobweb diagram for a better comprehension of the 2.0 network representation in the tangible reality.

Starting from the idea that, succinctly, a social network stands for a finite set or finite sets of actors connecting to each other, it follows that social network analysis implies detecting and interpreting the social patterns of the characteristics that bring actors together, all of these being represented graphically by means of the already mentioned programs (Everton, 2013, p. 9).

Such an example of a program is UCINET developed by Linton Freeman when he was teaching in the University of California. The name of the program, Irvine, was derived from this place; this program was afterwards upgraded several times. This is one of the best known social network analysis software and also most used as it incorporates a series of measuring tools for data provided by social channels as well as other data management tools. All these contribute to estimating measurements of the network topography, giving information on the central actor of the network, identifying subgroups and estimating the measurement values of the structural equivalence of the considered platform.

Moreover, UCINET provides several tools for data subset selection from the network and for data import and export in any format; all these features make of UCINET a powerful program used in social network analysis.

Conclusions

Accordingly, it may be concluded that the use of software intelligence based on a 2.0 dimension, through social media analysis, creates numerous opportunities that could be utilized by intelligence officers to obtain additional information for an investigation topic and sometimes to obtain new aspects on the information which could not be observed by the field officers. In this context, if the implementation of INTs 2.0 is supported, their utilization

could offer the missing pieces of a puzzle which direct the activity the intelligence services (Everton, 2013, p. 50).

However, one should take into account the simple fact that those who use social media for purposes that do not serve the values and national interests, could become aware of these opportunities and that they could become the first beneficiaries of them; therefore social networks and the internet remain an area to explore, a demilitarized zone where both groups wishing to affect the security environment and the intelligence services are acting and fighting for digital supremacy. The question arising from this situation can be formulated then as: how much risk is each one willing to take to conquer the digital sphere?

Will the intelligence services be ready to carry out a new research and knowledge activity in order to understand the new phenomena or will these groups protect their leaders, sympathizers, methods so well that the international intelligence community would fail to collect the necessary data? While taking into consideration the above mentioned opportunities and the emerging activities undertaken by groups that can produce threats to national, regional and international security and affect the values and the interests of the states and of non-state actors as well as the continual fight between the intelligence community structures and these groups, one cannot and must not lose sight of the fact that there are limits for the data collecting activity via social media intelligence.

References:

1. Ciupercă, Ella, Ciupercă, C., Niță, C, Stoica, M., (2010), *Rolul rețelelor de socializare pe internet în modelarea comportamentelor*, București: Editura ANI.
2. Everton, Sean, (2013), *Disrupting Dark Networks*, Cambridge University Press.
3. *Financial Review*, available on www.afr.com/p/technology/google_glass_and_social_media_to_R5en8jIWOeVUjasiJqsaIL.
4. *How riot rumours spread on Twitter*, (December 7, 2011), în *The Guardian* available on www.theguardian.com/uk/interactive/2011/dec/07/london-riots-twitter.
5. Le Bon, Gustave, (2012), *Psihologia mulțimilor,* București, Editura Antet.
6. Lesidrenska, Rada, Bancheva, Vessela, (2012), *Adaptation of Intelligence and Security Services to Contemporary Challenges* în Proceedings of the XVIIIth International Conference – Intelligence in the Knowledge Society.
7. Lewis, Paul, (August 7, 2011), *Tottenham riots: a peaceful protest, then suddenly all hell broke loose*, în *The Guardian,* available on www.theguardian.com/uk/2011/aug/07/tottenham-riots-peaceful-protest.

8. Maior, George Cristian, *Mesajul directorului Serviciului Român de Informaţii* în *SRI în era informaţională, Viziunea strategică 2011-2015*.
9. *Mark Duggan inquest and reaction*, BBC News accesibil pe www.bbc.com/news/uk-england-london-25648913.
10. *Pagina oficială de facebook R.I.P. Mark Duggan* available on www.facebook.com/pages/RIP-Mark-Duggan/200659976657547.
11. Philips, Richard, Frost, Diane, Singleton, Alex, (2012), *Researching the riots* în the Geographical Journal.
12. Sir Omand, David, Bartlett, Jamie, Miller, Carl, (2012), *Introducing Social Media Intelligence,* în *Intelligence and National Security*, Vol. 27, Nr. 6.
13. Sir Omand, David, Bartlett, Jamie, Miller, Carl, (2012a), *A Balance between Security and Privacy Online Must Be Struck*, în Demos.
14. Social Media Intelligence (SOCMINT), (October 31, 2012), Same Song, New Melody?, available on www.osintblog.org/2012/10/31/social-media-intelligence-socmint-same-song-new-melody.
15. Surowiecki, James, (2005), *The Wisdom of Crowds*, Anchor Books.
16. *Use of Internet for Terrorist Purposes*, (2012), Oficiul Naţiunilor Unite pentru Droguri şi Criminalitate.
17. Wright, Paul, (June 26, 2013), Meet Prism's little brother: Socmint, available on www.wired.co.uk/news/archive/2013-06/26/socmint.