Journal homepage: www.jmisci.com
Contact: jmiseditor@gmail.com

Journal of Military and Information Science
Institute of Science

Special Issue,
International Conference on Military and Security Studies,ICMSS-2015

Report

How to Make Social Media More Effective as an Exploitation Area?

C.Arslan *, M.Yanık **

* Turkish Army War College, , İstanbul, Turkey arslancetin157@gmail.com
** Turkish Army War College, Department of Operations and Intelligence, İstanbul, Turkey, muratyanik76@gmail.com

‡ Corresponding Author; Address: Tel: +90 398 01 00, e-mail: arslancetin157@gmail.com

Abstract- The immediate rise of social media has made a big change in the habits of communication. All the applications like Facebook, Twitter, Google+ and LinkedIn have gained a wide range of usage allowing the applicants have a very media to express themselves freely. The users of social media have a chance to articulate themselves, share their views and interact with the other. These opportunities also enable the intelligence workers to reach some information that is not possible to catch when directly asked for or cannot be dared to ask indirectly as it is not appreciated. Because, in social media, all the contents are built by the users willingly and the users of social media don't feel themselves under threat as they build up the content without external push. So it is not possible to talk about privacy. Although some contents have limited access, when the size of unlimited ones are thought, social media presents a big opportunity for data mining. In today's intelligence literature, social media is a subject of Open Source Intelligence (OSINT). This study tries to explain how to use social media more effectively as an exploitation area for intelligence staff.

Keywords- Data Mining, Exploitation Area, Open Source, Social Media, Opportunity.

1. Introduction

Using social media is among the most common activities of internet users of all ages and, today, millions of people are dealing with it. Although there are many definitions made for social media, generally, it can be defined as "a group of internet-based application that builds on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user generated content". (Andreas & Haenlein, 2010) In the last decade, social media (e.g., blogs, social networking sites, wikis, video and photo-sharing sites, etc.) has expanded rapidly and transformed the ways of interaction between individuals. (Fischer & Reuber, 2011) Their unique characteristics which let people interact freely and limitlessly among themselves, have attracted great attention from general public all over the world. Introducing some opportunities, social media has changed the way and form of communication between organizations, communities and individuals. Its quality, extension, frequency, usability, immediacy, promptness and permanence have made a real difference from the traditional ones. Today, among the most popular ones are Facebook, Twitter, Linked In, Pinterest and Google Plus+. (Top 15 Most Popular Social Networking Sites , 2014) According to statistics, the largest online social network Facebook has 1.4 billion users worldwide. (Statistics, 2014) Social media has made a long way in a very short time since its emergence approximately two decades ago and seem to go ahead evolving and attracting more people. So the social media has become a real global phenomenon.

Social media presents users a huge comfort in communication, letting them transfer their interactions, identities, arguments, views and even their emotions. As people upload more of their lives onto social media sites, they become more open to public and therefore more of a part of the public. Understanding the content of social media presents an opportunity for intelligence services to pull necessary info. Because, while the users express themselves in some way, to some extent and at different times, they also give a piece of information they don't want to share when directly asked for. Social media makes it possible to collect overt and covert information and to convert them into a much more meaningful knowledge by analysing them when the

specific tools, specially made to collect and analyse information, are used.

On the other hand, social media spaces are also a subject of state security and public safety. To set an example, it is a fact that Facebook has been used as medium to commit crime as to hire hit men, groom the targets of paedophiles, violate restraining orders, steal identities and fatally cyberbully victims. So, when we evaluate the social media comprehensively, it is totally clear that the social media has a big place in the lives of people and is an important subject to both criminals and security services.

In this study, in part two, the term of Knowledge Development (KD) and its relation with Intelligence will be explained. In part three, the place and the importance of Open Source Intelligence (OSINT) in KD will be portrayed. After highlighting the opportunities presented by social media in part four, a comprehensive comparison will be made between social media and OSINT in part five. In conclusion, it will be explained that social media intelligence is an expertise apart from OSINT and social media intelligence has to be categorized in a totally different intelligence discipline out of OSINT.

2. Knowledge Development (KD)

Before arguing the place of social media in Intelligence, it will be useful to shed lights on the term of KD. KD is defined as a process that includes collecting and analysing, and integrating isolated data into useable bodies of knowledge, and making that knowledge available so that it can be shared. (Bi-Strategic Command, Knowledge Development Concept, 2008)

KD is also driven by information and knowledge requirements relating to potential areas of strategic interest just before a crisis. The primary purpose of KD is to support subsequent decision making in response to indications and warning of an emerging security problem as well as during the planning, execution and assessment of operations. (Bi-Strategic Command, Knowledge Development Concept, 2008) The challenge in KD is to obtain the required information and make it available in a form that can be analysed and distributed timely.

KD provides the commander and their staff with a comprehensive awareness and understanding of environments.

2.1. Knowledge Development Process

An iterative process that supports planning, execution, and assessment, KD concept identifies three key steps in the process: A simple KD process is shown in Fig.1. (Bi-Strategic Command, Knowledge Development Concept, 2008)

- **Collection:** It involves the acquisition of information by various tools.
- **Analysis:** The purpose is to put information into context and then draw conclusions, deductions or implications. Analysis is required to obtain products for assessment, planning and execution.
- **Access:** It is about transferring the developed knowledge to the user or users by pushing or pulling, depending on the situation and operational requirement.

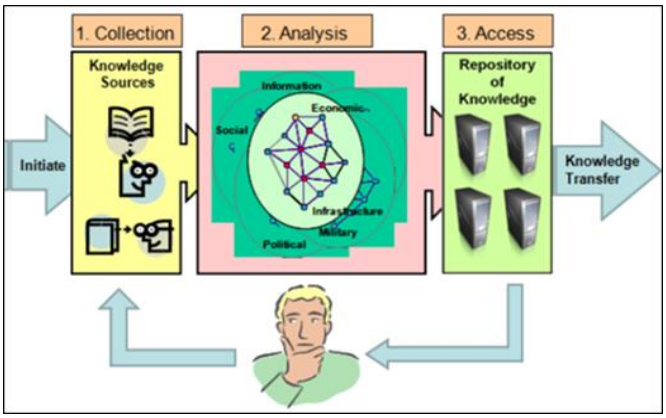

Fig. 1: The Knowledge Development Process Overview

2.2. Knowledge Development and Intelligence.

Both the terms of KD and Intelligence have close meanings. In order to make the terms clear, it might be useful to compare them. Intelligence can be described as the ability to perceive or obtain information and apply it to itself or other instances of information creating referable understanding models of any size, density, or complexity.

In military literature, intelligence is defined as the product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. (JP 2-0 Joint Intelligence, 2013)

Intelligence process is applied to support commanders and staffs in obtaining situational awareness and understanding of the three effective factors; threats, terrain and weather, and civil considerations. The main role of intelligence is to support commanders and decision makers.

Both the knowledge development and intelligence process are used almost in the same meaning. Although

there are some similarities between military intelligence process efforts and KD, they bifurcate in some different points.

The first one is that intelligence activities are focused primarily on actual or potential adversaries within a specific country or region. But in KD, not only the adversaries are on the target but also all other key actors having possible affects directly or indirectly on the protected. In KD process, all the information and knowledge regarding the capabilities, interaction and influences of all actors are tried to be drawn.

The latter is that KD encompasses the deliberate use of non-military sources beyond the scope of military intelligence activities.

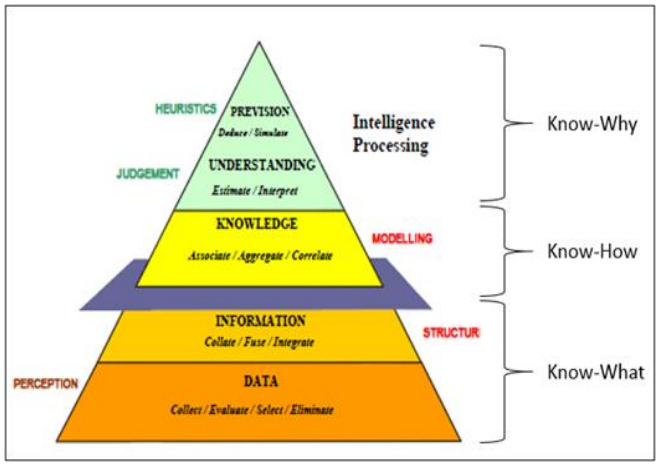

Fig. 2: The Knowledge Pyramid.

Looking at two differences, it is quite significant that KD comprises a larger area than military when compared to military intelligence. In Fig. 2, The Knowledge Pyramid depicts the relationship between Knowledge and Intelligence. (Biermann, 2004)

2.3. Intelligence Disciplines

To produce intelligence, firstly, the required information concerning foreign nations, hostile or potentially hostile forces have to be collected. To collect the required information there are many disciplines.

Each one of the disciplines of collecting required information to produce intelligence has its own characteristics in costs, sources, methods and targets, making it superior or weak when compared to the others.

In military literature, those disciplines are listed as Geospatial Intelligence (GEOINT), Human Intelligence (HUMINT), Signals Intelligence (SIGINT), Measurement and Signature Intelligence (MASINT), Technical Intelligence (TECHINT), Counterintelligence (CI) and Open-Source Intelligence (OSINT). (JP 2-0 Joint Intelligence, 2013)

Although it has not been shown a great respect, OSINT has close ties and collaboration with the other disciplines and on some certain areas, OSINT is irreplaceable. To evaluate the place of social media intelligence in OSINT, firstly, OSINT must be understood well.

3. Open Source Intelligence (OSINT)

Intelligence is crucially important to the military. And for the intelligence, collection, analysis and dissemination phases are the most sensitive areas. Mostly for the collection of the information, the procedures are centered on a highly classified basis and traditionally, intelligence services have concentrated on classified sources for their analysis. So, open source intelligence has been given little importance.

But by the time passes, open source data has been increasingly important to support the intelligence function. Especially getting higher and higher ability to skillfully mine data from a large, incoherent series of sources, has allowed analysts to build up detailed composite pictures of their area of interest.

The progress in information technology has made open sources more accessible, ubiquitous, and valuable. Anyone can gather open source intelligence much more easily and almost at no cost than ever before. Open sources have been getting increasingly easier and cheaper to acquire in recent years. The development in the Internet has provided us with many web sites where exists endless data stream.

Moreover, the progress in the Internet caused lots of changes in local radio and television broadcasts. Now they can be found on the World Wide Web where there is no need for any kind of expensive infrastructure of antenna or other equipment.

Today, open source has expanded well beyond "frosting" and comprises a large part of the cake itself. It has become indispensable to the production of authoritative analysis."(Gannon, 2001) Another explanation shows us the extension of OSINT has reached. The Director of CIA, Allen Welsh DULLES, has explained that the huge amount of public information, more than 80%, used by CIA is obtained from open sources. (Friedman, Open Source Intelligence, 2002)

Prior to Open Source Intelligence (OSINT), it might be beneficial to explain some terms: “Open Source” and “Publicly Available Information”.

Open source is any person or group that provides information without the expectation of privacy-the information, the relationship, or both is not protected against public disclosure. (ATP 2-22.9 Open Source Intelligence, 2012) Open sources refer to publicly available data with no limits to physical persons.

Publicly available information is data, facts, instructions, or other material published or broadcast for general public consumption; available on request to a member of the general public; lawfully seen or heard by any casual observer; or made available at a meeting open to the general public.(ATP 2-22.9 Open Source Intelligence, 2012)

When we come to OSINT, in military literature, it is defined as "the intelligence discipline that pertains to intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence and information requirement." (ADRP 2-0 Intelligence, 2012) Published or unpublished reference, unofficial and draft documents, material, research, or 'cloud' databases, and web-based networking platforms or repositories are of examples of open source.

It would be beneficial to state what is said by General Sam Wilson, USA Ret. former Director, Defense Intelligence Agency (DIA) to understand the importance of open source in intelligence. For him, "Ninety percent of intelligence comes from open sources. The other ten percent, the clandestine work, is just the more dramatic. The real intelligence hero is Sherlock Holmes, not James Bond".(Friedman, 1998) Nowadays, previously neglected open source intelligence is shown great respect.

OSINT supports warnings, tips, and cues other intelligence disciplines, and provides the context for understanding classified information. It can also reduce large target sets, quickly filling information gaps.

OSINT is no replacement for covert collection. Open sources increasingly enhance secret collection programs. Many intelligence services benefit from the growing volume of open data. OSINT allows covert collectors to organize limited resources for the most complex problems.

Although many people don't consider OSINT as intelligence, open sources, which are so accessible and valuable, have a very important place in Intelligence Community and almost more than half of the required information collected from OSINT.

The intelligence process (ATP 2-22.9 Open Source Intelligence, 2012) that consists of four steps (plan, prepare, collect, and produce) and four continuing activities (analyse, generate intelligence knowledge, assess, and disseminate) results in knowledge and products about the target. OSINT makes the intelligence process go further and supports it.

OSINT is also both a force and a resource multiplier. (Steele, 1995) OSINT provides practical advantages in politics and military, which complement the gaps of traditional intelligence. Being fast and available at low cost makes it indispensable.

To conduct OSINT exploitation, the areas primarily focused on are those: (ATP 2-22.9 Open Source Intelligence, 2012)

- Public speaking forums.
- Public documents.
- Public broadcasts.
- Internet web sites.

Above are the sub-categories of open source intelligence. And also we can call them as the exploitation areas of OSINT.

Public speaking forums are about speaking held publicly like meetings of political leaders. Acquiring information, according to information collecting plan, at public speaking forums, requires being careful not to violate the laws banning the unauthorized collecting of info. The three components of public speaking forums are speaker, audiences and the format of public speaking.

Public documents are about any kind of papers having text on it. For the public documents, once collected, they are analysed and the information obtained is sent to intelligence community. The components in public documents are printed, recorded and graphic ones.

Public broadcasts searches enable deployed organizations to collect and process information from international and national broadcasts that are of interest. The components of this area are TV's and radio channels.

For OSINT, It can be asserted that the most comprehensive exploitation area is the Internet. Internet has a close relation with social media. It is the main infrastructure for social media. Without Internet infrastructure, we cannot talk about social media and its applications. In the Internet, a wide range of information is collected, processed, and produced, enabling the dealer to provide great opportunities.

When the list about the OSINT exploitation areas is checked, all of the areas, out of internet web sites, have

a long history and exposed to evolution with the emergence of internet web sites. Because, today, all the documents, speaking and broadcasts uses the Internet media to reach a broader group of people or to benefit from facilities in infrastructure presented by it. For example, via Internet, a conference held locally can be broadcasted all over world instantly and cheaply or TV and radio broadcasts are done by the help of Internet, making it unnecessary to make very expensive investments for the broadcast equipment. All kinds of documents are accessed easily all over the world, generally with almost no publishing expenditures.

So, today all the exploitation areas seem to be depended closely to Internet media but that doesn't make those areas worthless. In spite of being depended to the Internet media, to collect and analyse information in order to obtain required knowledge, each of them has their own methodology and approach different from social media in the Internet world.

OSINT exploitation typically gathers and receives information, performs research, and reports and disseminates information to make intelligence products. The products of OSINT can be categorized according to their purposes and area of use.

In military, the categorization of OSINT product can be listed as Indications and Warning Intelligence, Current Intelligence, General Military Intelligence, Target Intelligence, Scientific and Technical Intelligence, Counterintelligence and Estimative Intelligence. The definitions of the categorized products of OSINT are given below. (ATP 2-22.9 Open Source Intelligence, 2012)

To speak of them concisely, Indications and warning are intelligence activities aimed to detect and report time-sensitive information about the developments that may involve threat in foreign country.

Current intelligence supports operations that continue. In current intelligence current threats have an important place.

General military intelligence is a kind of intelligence that concerns military capabilities of foreign countries or organizations or any other entities affecting potential military operations relating to armed forces capabilities.

Target Intelligence is something that determines the vulnerability and importance of target and locates the components of a target or target complex.

Scientific and technical intelligence is about obtaining scientific and technical information of a foreign country by collecting, evaluating, analysing, and interpreting. Counterintelligence covers information collected and activities managed to identify, exploit, deceive, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted on behalf of foreign.

Estimative intelligence identifies, describes, and forecasts adversary capabilities and the implications for planning and executing military operations.

In policing, the areas of OSINT can be listed in three categories by adapting from "Policing in an Information Age". (Bartlett, Miller, Crump, & Middleton, 2013) Those are Engagement, Enforcement and Intelligence.

The police use open source media as a means for engagement with the public. As they supply a high interactivity, social media is the very environment to reach rapidly rumours about what is thought as a result of events. When used as an engagement tool, social media allows the police to make constant contact with the public and to inform them accurately sharing correct information about rumours.

At the same time, engagement with the public makes the police more alert and vigilant as a result of high situational awareness. Because this kind of engagement triggers the flow of valuable information from public to the police.

Open source media, especially social media, are crucially important a public area where illegal actions can be both made and detected. Consequently, that provides new sources of collecting information and evidence for criminal investigation and prosecution. While those media are providing new sources for evidences, it shouldn't be forgotten that they also provide a new area to commit unique crimes subject to public law.

The provision of legitimate, timely, decisive and robust intelligence obtained from open sources can contribute decisively to public safety. TV's, radios, newspapers, and especially social media let the dealer obtain valuable information that supports intelligence. For social media, some analytic and big data acquisition tools may help the police focus on emerging events by supplying valuable intelligence.

After giving general information about OSINT and its place in the Intelligence, contributions of social media to the Intelligence can be understood better.

4. Social Media in OSINT

As mentioned above, there are lots of definitions about social media. Each one of different definitions

gives some clues about what social media is and not. According Bruce LINDSAY, an analyst of the US Congressional Research, "the term of social media refers to internet based applications that enable people to communicate and share resources and information. Social media can be accessed by computer, smart and cellular phones, and mobile phone text messaging (SMS).(Lindsay, 2011) In this definition, the aim and the means of the social media are emphasized.

An expert on strategic communication, Prof. Bobbi Kay Lewis from Oklahoma State University makes another definition to social media. For her, "Social media refers to messages created and disseminated through digital, mobile and Internet-based technologies. Social media are the creation of platforms that connect people together, provide an opportunity to produce and share content with others, extract and process community knowledge and share it back. (Lewis, 2009) In her definition, in addition to the means, communication and knowledge dimension of social media is highlighted. Although there are many kinds of definitions, none of them is wrong. Each of the definition puts emphasize on some characteristics already owned.

To understand the extension that the social media has reached, it would be useful to share some general information. Internet and mobile technologies have been the propellant of the rapid expansion of social media, providing infrastructure for content generation, information dissemination, and communications. About 3 billion people use Internet sites, blogs and forums to post, share and view content. (World Internet Usage and Population Statistics, 2014) Although social media may not be publically viewable, basically the logic of social media requires it to be open, at least to the certain public that was defined by the user. The most well-known are Facebook, Twitter, LinkedIn, Pinterest and Google Plus+. Social media accounts for an increasing proportion of time spent on-line. Facebook users spend 9.7 billion minutes on the site, share 4 billion pieces of content a day and upload 250 million photos. (Barlett & Carl, 2013)

As social media has presented many opportunities and been already a critical part of the information space, social media platforms and its applications gained rapidly a widespread adoption from all walks of life. From business world to politicians, from policing services to military, every part of life take place in social media. While business world use social media as it is a rich source of information and a platform for innovation or design business. Today, social media is irreplaceable for business world for public relations (PR) and marketing.

For politicians, political parties, and governments, social media presents a big opportunity for feedback of applied policies, instantly.

For intelligence analysis communities and homeland security, social media presents immense opportunities for some areas. To learn about a terrorist group's behaviour or public opinion on applied policies of a hostile country are among benefits of social media.

Availability of large scale of information and the ability to access it with almost no cost, presents big opportunities for intelligence services to gather information analyse it to produce useful intelligence via some well-designed and developed analyse tools.

Analyse tools are very important components of intelligence. Because, they are key factor that produce required intelligence from immense information space gathering small pieces of information and converting it into a meaningful context. But, of course, only analyse tools cannot solve the problem by itself. To exploit this information space more productively, there are some more steps like building up special units having expertise on this area, assigning well-educated staff and allocating some more budget.

In today's literature, the types of Social Media Intelligence (SOCMINT) can be divided into four categories: (Bartlett, Miller, Crump, & Middleton, 2013)

- Open source SOCMINT: In this type, all the intelligence is collected from publicly available sources Private information can be collected only when the uploader let happen. Interception and deception is not among the collecting methods.
- Covert Directed Surveillance SOCMINT: This type of intelligence requires a legal authorization for the collector as private information about a person is taken from public domain.
- Covert Human Intelligence Sources SOCMINT: This type also requires legal authorization. It is classified when a person aims to get access to information about another individual using social media.
- Intercept/Covert/Intrusive Surveillance SOCMINT: Intelligence gathered from social media that makes available the content of a communication, while it is being transmitted, to a person other than the sender or intended recipient, by monitoring, modifying or interfering with the system of transmission. This type of SOCMINT requires the highest level of authorization.

With some challenges and restrictions, social media, today, is one of the most important sources of intelligence. It seems to gain more importance increasingly as the usage of social media gets more widespread. Today, it is quite normal to debate the place of social media in OSINT, especially after understanding the contributions of it the Intelligence.

5. Discussion about the Place of Social Media in OSINT

In today's literature, social media is an area to be exploited under OSINT. In Fig. 3, below, the place of social media in Intelligence is illustrated. (ATP 2-22.9 Open Source Intelligence, 2012)

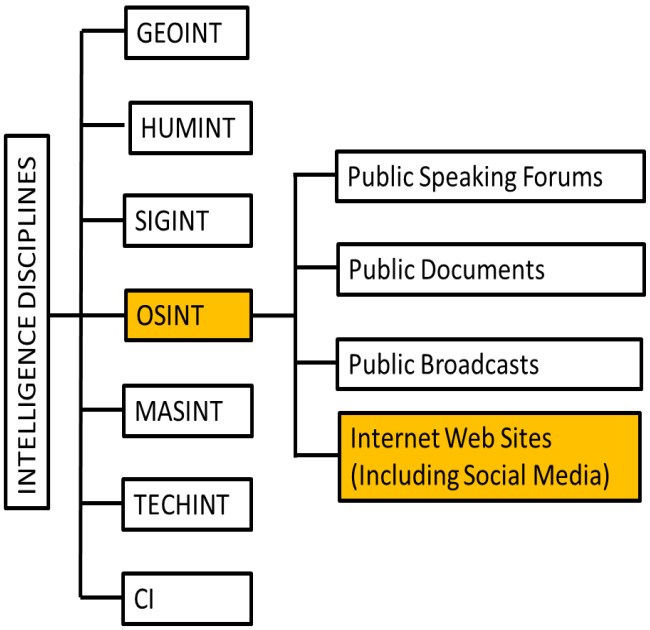

Fig. 3: The Place of Social Media in Intelligence Disciplines

When we compare the sources of OSINT, we realize that internet-based sources have gone far beyond the other sources like TV and radio broadcasts, documents or public speaking.

Although the areas out of Internet web sites, have caught a new wave by digital age, it only changed the form of the sources and the level of accessibility, making them much more useful for collecting data for intelligence producers.

But the emergence of social media has made a dramatic change in perception of OSINT. Social media that is seemed as an inseparable part of Internet, uses Internet just as an infrastructure and offers too much more than web sites. In Table 1, the comparison is shown between OSINT and SOCMINT on some certain areas.

To compare OSINT and SOCMINT, some factors are to be considered. In Table 1, those factors are gathered under the titles of "source", "collection", "crux" and "source protection" in a general view to see the main differences between them.

Table 1: Comparison Between OSINT and SOCMINT

	OSINT	SOCMINT
SOURCE	Publicly available	Social media
COLLECTION	Overt	-Overt, - Covert, - Intrusive.
CRUX	Identifying related and reliable Info.	Interaction
SOURCE PROTECTION	N/A	- Covert - Intrusive (If necessary)

As it is seen at the table 1 (Bunnik, 2014), while the access to social media sources may require permission, the main source of OSINT is publicly available.

All of the sources of OSINT present overt information. Overt information, of course, is also valuable for producing intelligence, but when compared covert ones, it is less promising.

In OSINT, by data mining, you can only reach the information given by the source like journalist, academician, or politician, limited in numbers. But in social media, the source is much wider and has much more variety, resulting much more attendance. As a result of interaction in social media, it is quite possible to collect some covert information given or shared unintentionally.

Social media, different from OSINT, presents some opportunities also. (David, Barlett, & Miller, 2012) Among the opportunities, "crowd-sourced information", "research and understanding", "near real-time situational awareness", "insight into groups", and "identification of criminal intent or criminal elements" are there.

As it is stressed before, the size of the participation of the public in social media, gives a tremendous opportunity to produce crowd-sourced information. At the same time, it is mostly a reliable source to have an idea about the perception of the public, instantly, creating situational awareness.

For military purposes or in policing, to learn about a group on target is much more quick and effective giving realistic results. And also, although it is erasable,

the ability to go back in time and reach the deleted information makes permanent traces to follow.

Consequently, social media itself has different characteristics and presents invaluable opportunities. Although it is considered as a part of OSINT, today, it promises too much to attract attention when compared to OSINT and should be re-categorized as in Fig. 4, below.

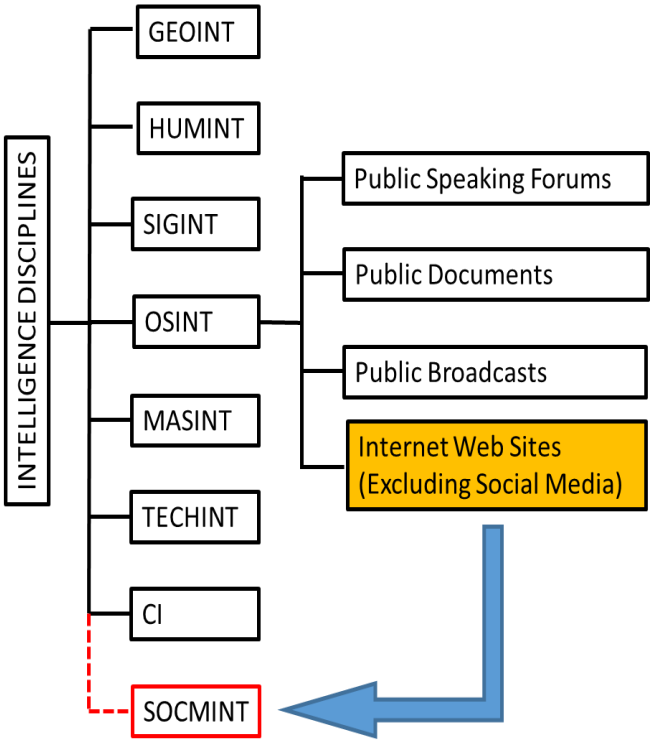

Fig. 4: Proposed Categorization of Intelligence Disciplines

5. Conclusion

Social media, after its emergence, has gained rapidly a widespread adoption from all walks of life and has taken a very important place in people's life presenting many opportunities in any area of communication. It seems to dominate any kind of communication means, as it is cheap, easy, effective and available on all over world.

OSINT, which had been argued once whether it was one of disciplines of intelligence or not, has gained an important place in intelligence world, depending on the opportunities presented by rapidly developing Internet infrastructure worldwide.

But, today, Internet and mobile technologies, which were an important part of OSINT at once, have been the propellant of the rapid expansion of social media, providing infrastructure for content generation, information dissemination, and communications.

Now, social media applications have turned to an environment that the big data of billions of people all around the world, streams constantly and uncontrollably.

This new phenomenon presents irreplaceable opportunities for the intelligence services in both military and policing. But to benefit from these opportunities, some amendments and regulations are to be made and some steps to be taken besides making investments on the technologies that supports collecting and analyzing data tools.

To state the required changes to be made to exploit social media for producing more effective and exact intelligence, the articles given below will be useful. To benefit from social media requires;

- Special units,
- Well-educated staff,
- Expertise on certain areas,
- Well-developed analysis tools,
- Legal and ethical framework and
- Its own (larger) budget.

Social media intelligence requires special units to produce intelligence professionally. As a specialized area, to be more effective and fruitful, it requires a unique team that deal with only this job.

Social media intelligence units needs well-educated staff. Because sometimes to produce a useful intelligence requires to collect and analyze complex and complicated information that looks far apart from each other at first sight.

Social media intelligence needs expertise on some certain areas. The people assigned to work on this area must be well educated accordingly. So, only educated and experienced staff can be successful. And as Social media is not only for intelligence but also for counter-intelligence and PR Works, expertise gains more importance.

While big data, growing fast, presents a big source of information to work on, at the same time, while making it hard to mine. So this fact makes the well-developed mining tools obligatory. In order to have efficient tools and infrastructure, making big investments is inevitable.

As an essential requirement of democracy, all the activities must be based on legal and also ethical framework. Thus, the insufficient legal infrastructure must be updated according to the new order to meet today's demands.

And of course, to make such big change and to maintain it will have a cost. It requires a big investment.

After all, today, the biggest obstacle in front of the social media intelligence is the unawareness of the opportunities presented by it. Once it is surpassed, all the required amendments and regulations can be made easily and fast.

In today's literature, social media intelligence is only a practice in open source intelligence. But when the opportunities are considered, it deserves more. To be categorized as a different discipline out of OSINT, as SOCMINT, in producing intelligence, will make it more productive while pushing the initiative of innovation, amendments and investments forward on this area.

Acknowledgements

This article is an extended version of the paper appeared in the Proceedings of International Conference on Military and Security Studies-2015. The author would like to thank to the organizers and the editor of this journal for their efforts.

REFERENCES

ADRP 2-0 Intelligence (2012), Headquarters, Department of the US Army.

Allied Command Transformation, "Bi-Strategic Command, Knowledge Development Concept (2008), Pre-Doctrinal Handbook.

ATP 2-22.9 Open Source Intelligence (2012). Headquarters, Department of the US Army.

Bartlett J., Miller C., Crump J. and Middleton L. (2013). Policing in an Information Age, CASM Policy Paper.

Bartlett, Jamie, and Miller C. (2013). The State of The Art: A Literature Review of Social Media Intelligence Capabilities for Counter-Terrorism.

Biermann J., et al. (2004). From Unstructured to Structured Information in Military Intelligence-Some Steps to Improve Information Fusion. FGAN-FKIE, Wachtberg Germany, .3-8.

Bunnik A. (2014, August). Opportunities and Ethics of SOCMINT: Practices for State Agencies in the Netherlands, Inaugural VOX-Pol Conference, Centre for Applied Research in Security Innovation (CASI) 29 Aug. 2014.

Fischer, E., and Reuber, A. R. (2011). Social Interaction via New Social Media :(How) can Interactions on Twitter Affect Effectual Thinking and Behavior? Journal of Business Venturing, 26, 1-18.

Friedman R. S. (1998). Open Source Intelligence, Parameters, 28(2), 159-165.

Friedman R. S. (2002). Review Essay – Open Source Intelligence, in NATO Open Source Intelligence Reader, Supreme Allied Command Atlantic (SACLANT), Norfolk VA, US.

Gannon J. (2001). The Strategic Use of Open-Source Information, Studies in Intelligence, 45(3), 67.

JP 2-0 Joint Intelligence (2013). Headquarters, Department of CJCS.

Kaplan, A. M. and Haenlein M. (2010). Users of the World, Unite! The Challenges and Opportunities of Social Media. Business Horizons, 53(1), 59-68.

Lewis B. K. (2009). Social Media and Strategic Communications: Attitudes and Perceptions among College Students. (Doctoral Dissertation, Oklahoma State University).

Lindsay, Bruce R. (2011). Social Media and Disasters: Current Uses, Future Options, and Policy Considerations, Vol. 41987. Congressional Research Service.

Omand, D., Bartlett J., and Miller C. (2012). Introducing Social Media Intelligence (SOCMINT), Intelligence and National Security 27(6), 801-823.

Social Networking Statistics, [Online]. Available: http://www.statisticbrain.com/social-networking-statistics/ Latest Access Time for the website is 29 December 2014.

Steele Robert D. (1995). The Importance of Open Source Intelligence to the Military, International Journal of Intelligence and Counter Intelligence, 8(4), 457-470.

Top 15 Most Popular Social Networking Sites, [Online]. Available: http://www.ebizmba.com/articles/social-networking-websites., Latest Access Time for the website is 29 December 2014.

World Internet Usage and Population Statistics, [Online]. Available: http://www.internetworldstats.com/stats.htm Latest Access Time for the website is 29 December 2014.