RESEARCH PAPER
No. 139

JANUARY

2010

HARRIS MINAS
(Intelligence Analyst in Sandstone S.A., Luxembourg)

CAN THE OPEN SOURCE INTELLIGENCE EMERGE AS AN INDISPENSABLE DISCIPLINE FOR THE INTELLIGENCE COMMUNITY IN THE 21st CENTURY?

RESEARCH INSTITUTE FOR EUROPEAN AND AMERICAN STUDIES (RIEAS)
 # 1, Kalavryton Street, Alimos, Athens, 17456, Greece
RIEAS url: www.rieas.gr

RIEAS MISSION STATEMENT

Objective

The objective of the Research Institute for European and American Studies (RIEAS) is to promote the understanding of international affairs. Special attention is devoted to transatlantic relations, intelligence studies and terrorism, European integration, international security, Balkan and Mediterranean studies, Russian foreign policy as well as policy making on national and international markets.

Activities

The Research Institute for European and American Studies seeks to achieve this objective through research, by publishing its research papers on international politics and intelligence studies, organizing seminars, as well as providing analyses via its web site. The Institute maintains a library and documentation center. RIEAS is an institute with an international focus. Young analysts, journalists, military personnel as well as academicians are frequently invited to give lectures and to take part in seminars. RIEAS maintains regular contact with other major research institutes throughout Europe and the United States and, together with similar institutes in Western Europe, Middle East, Russia and Southeast Asia.

Status

The Research Institute for European and American Studies is a non-profit research institute established under Greek law. RIEAS's budget is generated by membership subscriptions, donations from individuals and foundations, as well as from various research projects. The Institute is autonomous organization. Its activities and views are independent of any public or private bodies, and the Institute is not allied to any political party, denominational group or ideological movement.

Dr. John M. Nomikos
Director

RESEARCH INSTITUTE FOR EUROPEAN AND AMERICAN STUDIES (RIEAS)

Postal Address:

 # 1, Kalavryton Street
Athens, 17456, Greece
Tel/Fax: + 30 210 9911214

E-mail: rieas@otenet.gr

RESEARCH PAPER
No. 139

JANUARY

2010

HARRIS MINAS
(Intelligence Analyst in Sandstone S.A., Luxembourg)

CAN THE OPEN SOURCE INTELLIGENCE EMERGE AS AN INDISPENSABLE DISCIPLINE FOR THE INTELLIGENCE COMMUNITY IN THE 21st CENTURY?

Table of Contents

Introduction

Since the end of the Cold War, societies have become more and more open. This openness of the world is a consequence of the information revolution which started at the end of the 20th century and its impact is obvious in our lives. Nowadays, we can be more easily, quickly and adequately informed about what is happening around the world. The intelligence community ought to adapt to this new environment and confront the new threats that emerge. This adaptation has to come along with the exploitation of all the sources available in its disposal. In this new era, Open Source Intelligence (OSINT) seems to have the potential to develop to the most well-suited intelligence discipline to confront the modern challenges. This does not necessarily mean that its role will surpass the one that clandestine disciplines have. It remains to be seen if OSINT could establish as an indispensable part of the intelligence process and as a vital contributor to the final intelligence product owing to its compatible nature with the global environment.

OSINT cannot emerge all of a sudden as the dominant intelligence discipline. This is a transitional period for it since it has to come out of the shadows of negligence and attract the attention that it merits. Thus, it is sensible why OSINT does not yet receive the same respect by the whole intelligence community as far as its utility and role is concerned. In this paper, I will make an attempt to focus on the reasons why OSINT tends to evolve as a sine qua non for the intelligence community in the 21st century.

Like the use of OSINT itself so far, the research on this subject is also limited. According to my viewpoint, OSINT will soon develop as a more interesting issue of research on intelligence studies because of its increasing importance. The lack of extended bibliography led me to get my background insight from some NATO publications on OSINT and, among others, from various articles of Robert Steele who is the founder of OSS.Net, an organization promoting OSINT importance. In addition, I conducted an interview with Avital Johanan who is an open source analyst at Jane's Information Group, a private intelligence provider. Using the tools I have in my disposal, I will try to argue in favour of the utility and role of OSINT in the 21st century.

In the beginning, I believe it is helpful to concentrate on some key background features of OSINT. Some definitions will make clear its distinct characteristics and its difference with simple open source data and open source information will be explained. Then, I will analyse the characteristics of the open sources intending to indicate their importance in the modern world and, consequently, in the emerging OSINT discipline.

In the second chapter, my analysis will focus on the producers of OSINT. Both of public and private nature, their increasing role manifests the respect that governments and private companies start to attribute to this discipline. In addition, the examination of OSINT products will indicate their compatibility with the modern needs. Finally, the difference between open and classified methods of collection and analysis will also become evident.

The applications those products can find will be examined in the third chapter. Trends that gradually appear can be demonstrated by the OSINT applications in governments, and specifically in the defence departments, and by OSINT applications in international organizations such as NATO and UN. The contribution of NGOs and the OSINT implementation in the business sector and in non-state actors' activities will also be searched.

In the following chapter, the benefits and drawbacks of OSINT will be compared. This will take place so that a holistic view is given for the OSINT and its suitability to the current international environment can be judged.

In the fifth chapter, the private sector capabilities will be demonstrated and a comparison to the ones that governments have will make clear some advantages and disadvantages. Furthermore, it will also be analyzed how they can integrate and bring better results.

Finally, in the sixth chapter, I will try to argue that the implications of the information revolution can facilitate the use of OSINT while the emerging asymmetric threats necessitate more vigilance and preparedness that OSINT can give thanks to its

attributes. Hopefully, at the very end of this research I will be able to support a new crucial role for OSINT in the intelligence process during the 21st century.

1. Introducing Open Source Intelligence: Definitions and Sources

Defining Open Source Information and Open Source Intelligence

The importance of OSINT is increasing and before moving to its producers and applications it would be beneficial to define it. In order to reach a definition for Open Source Intelligence (OSINT), it is essential to firstly define the terms of Open Source Data (OSD) and Open Source Information (OSINF) which constitute the raw material for the creation of the OSINT. The clarification of the differences among these terms is useful since it will illustrate that OSINT is not just simple information that anyone can find in the public domain. After this necessary background information, an attempt will be given to present the most substantial open sources available in the hands of OSINT analysts.

Relying on the definition given by the NATO Open Source Intelligence Handbook, Open Source Data (OSD) can be the raw print or oral debriefing of a government official, a librarian or a journalist with expertise on a specific area; it can also be a personal letter or any other form of information from a primary source. It could also be obtained from technical sources like a photograph, a tape recording or a commercial satellite image.'[1] OSD is data that has not been processed and no editing by analysts has taken place. It is the raw data that needs to undergo some elaboration in order to reach the next level which is the OSINF.

This means that the product from primary sources can be transformed in OSINF when being analysed, edited, filtered and validated in a certain level and then disseminated on Internet, newspapers, radio or TV broadcasts, academic journals, government reports, etc.[2] Recently, blogs have also become an area from which intelligence analysts can get information about the social perspective and the general feeling of

[1] NATO OSINT Handbook (2001), p.2
[2] NATO OSINT Handbook (2001), p.2

societies.[3] All these are secondary sources which constitute the OSINF and they are less expensive to be obtained by the public comparing to the primary or technical sources which are not published literature. Apart from that, OSINF as generic information is disseminated to the broad public in a much easier way than the primary sources and almost everyone can find the information he is interested in. However, this is not always the case because grey literature is also a part of OSINF and it refers to material that cannot be acquired easily although not hidden. Conference proceedings, dissertations or in-house newsletters are some examples of grey literature and people who want to draw information from these sources should know how to access them.[4]

When it comes to the definition of Open Source Intelligence (OSINT), it is difficult to fit every aspect of it in a single definition since OSINT has a lot of features that makes it different from OSD and OSINF. It is vital to be said that the information that has been made publicly available has no value as intelligence product if it is not carefully selected, analysed, filtered, validated and then disseminated as a tailored product to a consumer on a timely basis.[5] This means that the intelligence analysts should be trained to discover the adequate sources of information. Then they should discriminate what information is proper to be used in terms of credibility, relevance and utility by the consumer. The distillation of information is also a necessity since from the big bulk of it, only some is needed for the tailored product and finally the dissemination to the right people at the right time is highly important so that the OSINT process offers to the intelligence field what its real potential is.[6] About the selected audience, whoever the consumer is -military commander, minister, president or businessman-, the tailored product should be targeted to deal with a specific question.

Plenty of definitions have been given in order to illustrate what OSINT is and how it can be acquired. Above, some key characteristics of OSINT were mentioned which indicate its difference with OSD and OSINF. Studying the definitions given by some

[3] Best & Cumming (2007), p.7
[4] Bowen (1999), p.50
[5] Ibid.
[6] The idea of using the four Ds (discovery, discrimination, distillation, dissemination) was taken by the chapter on open source intelligence cycle in the NATO OSINT Handbook.

prestigious bodies like NATO, the American Congress and the OSS Academy, it is helpful to discern the special attributes of OSINT although each one of them give special emphasis to different features.

Firstly, starting from the OSS Academy, a corporation founded by Robert David Steele to promote international understanding of the significance of OSINT, it provides the following definition:

> OSINT results from the integration of legally and ethically available multilingual and multimedia sources, with the heretofore largely secret processes of national intelligence: requirements analysis, collection management, source validation, multi-source fusion, and compelling presentation.[7]

In this definition, it is made clear that the processes which apply for the clandestine sources in the intelligence cycle should also apply for the open sources in order to acquire the open source intelligence. Thus, OSINT contributes to the all-source intelligence product. What is more, great emphasis is given to the legal and ethical way of information acquisition. Contrary to the human or signals intelligence techniques, open source information needs no clandestine collection methods to be obtained but its acquisition takes place only under the copyright constraints and commercial requirements when the vendors apply them.[8] Furthermore, OSS cast emphasis on the multilingual nature of open sources which is one of the main features of OSINT process and focuses on their availability in various electronic formats such as audio, text or video.

Secondly, another definition provided by the United States Congress in the 2006 Defence Authorization Act clearly sets what OSINT is:

> OSINT is intelligence that is produced from publicly available information collected, exploited, and disseminated in a timely manner to

[7] Steele & Lowenthal (1998a), pp.4-5
[8] Lowenthal (1998), p.1

> an appropriate audience for the purpose of addressing a specific intelligence requirement.[9]

The nature of OSINT is highlighted here as a form of publicly open information which after being subject to the stages of the intelligence cycle, it can turn into useful intelligence for the specific needs of the targeted user. The main features of OSINT are made clear such as the public sources, the need of information processing and the requirements at the last stage of dissemination.

Thirdly, another working definition to be mentioned is this of NATO:

> OSINT is information that has been deliberately discovered, discriminated, distilled, and disseminated to a *select* audience, generally the commander and their immediate staff, in order to address a *specific* question. OSINT, in other words, applies the proven process of intelligence to the broad diversity of open sources of information, and *creates intelligence*.[10]

In contrast to the Congress's definition which offers to the OSINT a status of intelligence discipline, the latter definition considers OSINT more as a 'foundation' for other disciplines.[11] Similarly to the previous definition, we can notice again the stages through which information is circulating. Here the 4Ds are used to give even more emphasis to this process but also an example is given about the select audience. Since it is a NATO definition and has a more militarily operational character, it refers to the commanders and their staff as the receivers of OSINT.

Sources of Open Source Intelligence

After having analyzed the main characteristics of OSINT which emanate from the various definitions it is substantial to examine in detail which are the sources that will provide the raw material for the production of intelligence. OSD and OSINF comprise the fuel for the OSINT and a quick reference of primary and secondary sources took

[9] Hamilton (2007), pp. 244-245
[10] NATO OSINT Handbook (2001), pp.2-3
[11] Hamilton (2007), p.245

place before. The rest of this chapter will focus on an effort to approach the most vital sources that constitute the ingredients for a successful recipe of OSINT. Among these sources one could include the media, the Internet, the commercial online sources, the grey literature, the commercial imagery and the human sources.

Before the advent and the expansion of Internet since the mid 1990's onwards, the media were the most widespread source that the few open source analysts of that era could use in order to extract useful information. However, media still remain one of the core capabilities of the OSINT activities since the monitoring of foreign print media like newspapers and periodicals as well as of electronic media such as TV or radio broadcasts will always be essential. Additionally, the recent technological evolution has contributed to the creation of online broadcast services that can be tracked and monitored like the electronic or print ones. There are both private and public sector information providers which can carry out this task. The two most prestigious ones are the Open Source Center (the previous Foreign Broadcast Information Service) and the BBC Monitoring Unit.[12]

In the recent years, it seems that golden nuggets can be acquired in an even less expensive and easy way because of the preeminent position that Internet has received. The World Wide Web has become a bottomless pool of publicly available information. As a result, this could not be left unnoticed by the intelligence services which try to exploit the benefits that Internet provides and transform the information available online in useful intelligence.

Internet is valuable because, apart from a provider of a huge bulk of information available to anyone, it is an ideal means of sharing information and communicating with partners, exchanging ideas, plans and professional insights. Furthermore, information sources on the Web can be immediately available either freely or after paying an access fee (subscription).[13]

Another feature Internet has as a comparative advantage in relationship to other open sources is the fact that one can acquire the information in a digital format and there is

[12] NATO OSINT Handbook (2001), p.5
[13] NATO OSINT Handbook (2001), p.6

no need of a human mediating factor to process it. Besides, Internet searches can provide specific information according to the desired characteristics of the search such as location, organization or other keywords that can render it more relevant and valuable for an OSINT analyst.[14]

Nevertheless, its vast nature is the undoubted characteristic. This can also be pointed out by the distinction between the surface and the deep web. On one hand, the surface web includes data and documents that are accessible via common public search engines like google. But this is only the 6% of what is stored electronically today and everyone can easily access and at no cost. On the other hand, the rest 94% of the stored information lies on the deep web which cannot be accessed by conventional search engines and includes premium online sources, specialized market research, corporate Intranets, private investigations, information broker services and geo-spatial information services. In order to search the deep web, a federated search should be conducted which can return results from intranets, web portals with subscription and private web sites and combine them with information from public sites.[15] That means that the invisible or deep web is located in searchable databases but only after a direct query is being done, the return of results from thousand of deep web sites can take place.[16] Since any interested side has the tools to dig on the web, it is certain that plenty of valuable information can be found and turned into practicable OSINT.

The commercial online premium sources were referred as a part of the deep web and of Internet in general but they deserve a separate reference since they are sources of high significance for the OSINT. The user should pay a subscription fee to gain access to these databases or to buy a specific online product. There are some very well-known leading services like Factiva, Lexis-Nexis and Dialog which provide access in various publications and archives like conference proceedings, dissertations or academic journals.[17]

There are also some more specialty commercial services like Jane's Information Group, Economist Intelligence Unit or Oxford Analytica which produce and sell more

[14] Umphress (2005)
[15] 'The Deep Web', http://osint.deepwebtech.com/about-deepweb.html , 5 July 2008
[16] NATO Intelligence Exploitation of the Internet (2002), p.50
[17] NATO OSINT Handbook (2001), p.7

specialized products. One certain feature of all these sources is the quality of their products in terms of currency, authentication, relevance, compiling the data and presentation management.[18] Since they consist of very experienced editorial teams, they operate in a competitive environment and their products are essential for various actors, any possible mistakes are inconceivable. Besides, their future directions and success rely on the feedback they receive from their clients. As a result, their importance for the various actors they provide with their services is substantial. The role of private firms in OSINT collection and function becomes obvious from the example of online premium sources but it will be discussed further in the following chapters.

Apart from the commercial publishers, the subscription agencies and the normal bookselling channels where useful sources for the OSINT can be discovered, there is also another source of information which is called grey literature. Grey literature is information that does not follow the normal proceedings of publication, distribution, control and acquisition but it is available through specialized channels or through direct local access and can be legally and ethically obtained.[19]

There are various producers of grey literature like research institutes, think tanks, trade associations, corporations, governments, political parties, academia etc. Common products that are considered as grey literature are usually government, technical and research reports, academic, conference and discussion papers, pre-prints and in-house newsletters. They are products for internal use and for restricted dissemination to partners, suppliers or vendors. As a result, if the Intelligence Community (IC) decides to collect material from these sources, some difficulties are raised because local databases and internal structures must be penetrated and the payment of a higher price compared to other open sources should be expected. [20]

As far as the utility of grey literature as a source of OSINT is concerned, it is very important for various reasons. First of all, grey literature can provide information to intelligence analysts that may never be published since some documents will never

[18] NATO OSINT Handbook (2001), p.7
[19] Ibid, p.8
[20] Soule & Ryan (2002), p.25

come out in public because they are directed for internal consumption. Moreover, grey literature can offer valuable information on a timely basis as long as conference proceedings or working papers may be published later in articles. In addition, some of the technical or government reports usually comprise very detailed content about specific issues such as a report on defence systems of allies or adversaries. As a consequence, when they are published they are less specialized since too many details in public may be avoided for security reasons.[21] It is made clear after all these advantages what grey literature may offer and that its use for OSINT can be of great value.

However, the collection of grey literature is more problematic than this of other open sources. It is a tough task to identify the suitable source in advance. For example, special networks are needed in order to detect interesting conferences before they take place. The value and the processing of grey literature are another two issues since this information is not always refereed and not in digital format but often in hard copy. Therefore, the retrieval and transmission of information become difficult tasks. Finally, in grey literature, the need for a multingual network of analysts is even more evident because a great load of information has to be retrieved from conferences, governments' papers and corporations' documents.[22]

The source with the most increasing value for OSINT seems to be the commercial satellite imagery. A few years ago, the countries that had satellite facilities were the privileged ones. Currently, every government or other national or international actors, who are willing to pay, have the ability to access satellite imagery. Since images of even remote regions can be available to intelligence services, this is an advantage to them because they can almost get through open sources what they were getting through spy satellites or not at all before.[23]

However, the significance of this source may also have some undesired implications. Firstly, an environment of 'mutually assured observation' among nations may develop and this will create a climate of suspicion. But since satellites provide only images

[21] ibid
[22] Soule & Ryan (2002), p.25
[23] Dehganzada & Florini (2002), p.40

and not intentions, the prudent use of this facility rests upon the users. Secondly, apart from intelligence services which possess a new open source tool in their intelligence warfare, other entities like NGOs, media or international organizations have also the same advantage. This could result in pressure against governments to undertake specific action stirred by these third parties.[24]

Last but not least, another very crucial source for the OSINT is the network of experts. There are remote places where secret services cannot go because of cost or distance or other reasons. The human contribution can be provided by external experts, internal experts or local knowledge and if all these three levels can be exploited, then the results will be positive. A network of analysts and on ground observers can prove very important and can provide very detailed analyses. Subject matter experts like journalists, employees of international organizations like inspectors for nuclear facilities or even indigenous people can contribute even more than a security cleared analyst. This is why networks of human sources on ground are much bigger than the case officers. [25] Consequently, with the most inexpensive way, intelligence services can use overt human experts to gain knowledge and information which will be current, relevant, valid and practicable to enter the intelligence processing cycle.

All those sources seem to provide great potential for the development of OSINT. It was made clear that OSINT is not just raw data available derived from those sources but all of them are valuable and should be managed and processed properly. This is how OSINT can have chances to develop further as an intelligence discipline.

[24] Ibid, pp.51-52
[25] Burke (2007), p.17

2. The producers of OSINT, their products and their methods

After having examined what Open Source Intelligence is and its sources, it is time to focus on who can turn all the available open source information into OSINT. I will make a distinction of OSINT producers. On one hand, we can find actors working for governments and funded by them such as the Open Source Center in U.S.. The BBC Monitoring Unit could be placed in this category since it mostly receives governmental funding and it is a valuable source of OSINT for the British government. On the other hand, private firms can be included as OSINT providers for intelligence agencies, government departments, international organizations and businesses. Some key examples are the Jane's Information Group, the Economist Intelligence Unit and Oxford Analytica. By presenting all those actors, I will try to seek the various kinds of products and services they can offer to the receivers of OSINT, and thus, OSINT's importance to them will become evident. Finally, the differences between OSINT and clandestine methods will be made obvious.

Government-based organizations

Open Source Center (OSC) founded in November 2005 by the Office of the Director of National Intelligence and its headquarters are located in the Central Intelligence Agency (CIA). OSC is the successor of the Foreign Broadcast Information Service (FBIS) which had been established in 1941 and its task was to gather information from foreign media and provide its products to the government.[26] Even though OSC is not a brand new service, its recent foundation indicates the attention that OSINT currently grasps in the US.

Regarding what OSC does in detail, a global network of multilingual analysts is maintained in more than 160 countries and they speak more than 80 languages. This network collects information for anything that the US government may be interested in. Those pieces of information vary greatly from military to local law enforcement issues and can be found on radio or TV broadcasts, on Internet, in newspapers, etc.[27]

[26] Best & Cumming (2007), p.12
[27] Director of National Intelligence Open Source Center, Appendix E (2006), p.E-2

Furthermore, as far as the role of OSC is concerned, according to its director's words Douglas Naquin, OSC pursuits a broader scope and function comparing to its predecessor. Consequently, OSC will not restrict itself to simply a provider of open source products and brokering services throughout the government. It aims to become a center which will not only give the opportunity to the customers to pull the information they need but also it will be able to push information to them. As Naquin says, 'we do not see this center as a monolithic big circle where everybody sends its requirements but as a hub.' [28]

Moreover, the OSC targets to give adequate expertise to a large number of open source analysts in order to make more feasible the exploitation of the vast amount of open sources. In addition, since OSC serves the whole American intelligence community, it seeks to expand its size in the following years. A combination of those two parameters -size and personnel training- can turn OSC into a real asset for the intelligence community and other government clients. As Naquin says, it is important to ask the right questions apart from trying to gather all information and it must be available to policy makers not only the information they want but also what they may need but they do not know yet. [29]

There is a variety of products and services that OSC can offer to its partners. Those are analyses, either short or long, depending on whether they concern real-time products or trends and patterns that media seem to follow. They may also be information related to the media such as the environment they operate, how they are used and by whom. Furthermore, key information can be gathered about important personalities that are connected with the media action and whose opinion influences governments, businesses and has impact on US interests. Another widely known task of OSC is its reports which include translations and transcriptions about political, economic or military issues and can be found on media, databases or internet websites. In addition, very crucial for customers of OSC are also the video services. Clients are given the possibility of pulling the information they wish among a huge data pool. Last but not least, OSC employs experts on geospatial technologies and a huge variety of maps and geographic data becomes available. All those services

[28] Ackerman (2006)
[29] Ackerman (2006)

constitute substantial prerequisites for the intelligence services' efforts to form their final products.[30]

BBC Monitoring has many common elements with OSC since they serve almost the same purpose with quite similar ways. The main difference is that BBC Monitoring does not belong to the British Intelligence Community. Its main function, however, is to provide the British government with its products and services. BBC Monitoring exists since 1939 and its continuous maintenance as a service indicates its utility for the British interests.[31] Administratively, it is a part of BBC but it is funded directly by its stakeholders and the principal of those is the Cabinet Office. Furthermore, it is an organization which can offer its product on a subscription basis and it is not limited to government officials like the OSC.[32]

Nevertheless, just like OSC, BBC Monitoring aim is to monitor the foreign media and provide its clients with global coverage through foreign channels which do not include only TV or radio broadcasts but also print media, Internet and news agencies. It maintains a vast network of sources in 150 different countries and from 100 languages. Its role is to transmit images, reports and 'the words as spoken' and provide foreign peoples' opinions and media in order to help any communities of interest back in UK.[33]

BBC Monitoring offers a number of products to its stakeholders. The first one is the 'International Newswire' which provides near real-time news coverage and the subscribers can access specific countries or topics they are interested in. There is also the 'International Reports Service' through which receivers get detailed and tailored reports on targeted countries and on subjects such as the armed forces status, weapons proliferation, technical, political and economic news. Moreover, media industry news are available and they concern emergence of new broadcasters, media restrictions, media trends or activities of clandestine broadcasters. Finally, there are also databases where clients can have access in specific archives or country profiles.[34] All these

[30] Director of National Intelligence Open Source Center Appendix E (2006), p.E-3
[31] Rotheray (2002), p.36
[32] http://en.wikipedia.org/wiki/BBC_Monitoring , 8 July 2008
[33] Rotheray (2002), p.36
[34] http://www.monitor.bbc.co.uk/index.shtml , 8 July 2008

products help governments keep track of various developments in foreign countries. BBC Monitoring provides various customers with these products but the private OSINT organizations usually have a broader spectrum of customers and most importantly, they receive no guidance from governments.

Private organizations

One of the most well-known private organizations and producers of OSINT and the most experienced one is Jane's Information Group since it operates from 1898 and has a vast network of clients; governments, military and commercial organizations. Being a very prestigious information provider and attracting clients from more than 180 countries, Jane's can provide timely and accurate OSINT, both in width and in depth, about markets, businesses, forces and geopolitics. This OSINT concerns mainly defence and security issues as well as the areas of law enforcement, public safety and transport.[35]

According to Avital Johanan from Jane's Information Group, the editorial team is the one who decides in which main areas the reports will be targeted and this board does not take orders from governments or businesses. Governments can buy some services as a whole and they exploit what they find useful. However, according to her, ad hoc teams take over the responsibility to prepare special reports tailored to the needs of customers but the editorial staff remains mainly devoted to the accomplishment of already commonly agreed products by the board. It is worth mentioning, though, that client's feedback is crucial for the function of Jane's as long as it helps the organization improving continuously and produce the OSINT that really is needed by the clients.[36]

As far as its intelligence solutions are concerned, Jane's offers 200 different products to its clients and a representative number of them will be presented here. I will focus on the defence and security sector products to project Jane's wide coverage. Regarding the defence products, government and armed forces can benefit from detailed analyses and forecasts on land, naval and air forces. More specifically these

[35] http://catalog.janes.com/catalog/public/index.cfm , 30 July 2008
[36] Interview with Avital Johanan from Jane's Information Group

products concern missile, ship, various weapons and nuclear capabilities as well as other structures. In the area of defence business, intelligence on forecasts, markets and global defence budgets are also provided.[37]

In the area of security, there are three levels where the analysts target. The first one is the country risk where Jane's provides information about specific dangers, risk of military coups, political stability, regional relations etc. The second one concerns the military capabilities and helps the receivers make their threat assessments. Last but not least, the terrorism and insurgency section offer deep insight about asymmetric threats, terrorism trends, terrorism financing and mitigation strategies.[38]

Plenty of more detailed products on the terrorism issue and on other ones are provided by the intelligence centres which offer to the clients OSINT about specific regions or subjects.[39]

Apart from those numerous products, Jane's recently succeeded to forge an alliance with ESRI. ESRI is a provider of geographic information system (GIS) software, technology and consulting and is the world's leading GIS supplier to the defence and intelligence community. Thanks to this development, Jane's will be able to add more maps and geographic information to its already competitive products and will improve the results and the services the clients get.[40] Consequently, it could be argued that Jane's capabilities as an information provider are very profound and scientifically challenging.

The same could be claimed for the Economist Intelligence Unit (EIU) which is a famous private organization targeting to offer economic, politic and business intelligence to its customers. This Unit founded in 1946, has more than 40 offices worldwide and covers 203 countries. It is a mainly business intelligence provider and a global partner of financial institutions, government agencies and international companies. Its aim is to help executives make the right choices by providing

[37] http://catalog.janes.com/catalog/public/html/defence.html , 30 July 2008
[38] http://catalog.janes.com/catalog/public/html/security.html , 30 July 2008
[39] http://catalog.janes.com/catalog/public/html/intelcentres.html , 30 July 2008
[40] 'ESRI and Jane's Information Group Forge Strategic Alliance' (2007), http://www.esri.com/news/releases/07_3qtr/janes-information-group.html , 31 July 2008

independent and punctual forecasts and analyses in three areas of business intelligence; country analysis, industry trends and management strategies. [41]

Focusing briefly to the services of EIU, the way EIU disseminate its intelligence can vary from meetings, electronic publications and executive programmes to presentations. As far as the products are concerned, they update the customers about recent developments and they can be disseminated through the viewswire or business newsletters. Furthermore, country reports, country profiles and country forecasts offer to the clients a comprehensive view about current trends on economic and political issues. There are also databases which inform them about more detailed questions on specific regions regarding the GDP, foreign payments or external trade, future investments and other economic indicators. Risk assessments is another essential service in clients' hands while there are also further information on industry trends and insight on various markets.[42]

Last but not least, Oxford Analytica is another private consulting firm which produces OSINT and established on 1975. It is another example of OSINT provider for international organizations, governments and private sector companies. While offering the same kind of services like risk assessments, political and economic trends and scenario planning, I would like to focus on its early warning unit. This unit developed a system which is called 'Global Stress Point Matrix'. The aim of this system is to follow some trends which indicate if some unlikely events may surprise the clients. In this way, it prepares them to mitigate the costs and to avoid a huge impact on their business. After some drivers and restrainers are defined, the analysts of Oxford Analytica can observe the 'stress balance' and the 'stress intensity' in their system and consequently they track down emerging trends.[43]

[41] http://www.eiu.com/site_info.asp?info_name=about_eiu&entry1=about_eiuNav&page=noads# , 14 July 2008
[42] Ibid.
[43] 'The Global Stress Points Matrix', http://www.oxan.com/GlobalStressPointsMatrix.aspx , 12 July 2008

Distinction of methods between classified and open sources

The last example of how private firms can produce OSINT can lead us to a comparison between the methods of OSINT producers and clandestine intelligence ones. Having examined both public and private OSINT producers, we can reach some conclusions about their efforts to collect and turn open source information into OSINT.

According to Avital Johanan, Jane's maintains contacts on the ground and those people have contracts with the organization. The editorial team and the experts on various issues are located in the organization offices around the world and they elaborate the information they receive adding their insight. Ms Johanan also noted the importance of the third parties reporting and other local media services which add their grain to the final products and she also stated that BBC Monitoring is one of Jane's partners.[44] Moreover, as we mentioned above, the cooperation with ESRI is also a supplementary source since Jane's can provide also geospatial information to its clients. In a very similar way, EIU works with experts worldwide apart from the country experts in the main offices. It also subscribes to electronic databases of organizations such as IMF, World Bank, OECD or UN to get statistics about various regions and compose reports.[45] Other private firms like Oxford Analytica or Stratfor work in the same way to produce their OSINT.

As far as the OSC and BBC Monitoring are concerned, they have a more governmental character but their methods of OSINT production do not vary significantly. One difference about them could be that they mainly focus on foreign media or news agencies and they do not collaborate with other types of organizations.

On the other hand, the usual methods with which the intelligence agencies collect their information vary in great extent comparing to OSINT services. There are both human and technical intelligence sources. As far as the human sources are concerned, there are intelligence officers in other countries where they operate under official

[44] Interview at Jane's
[45] 'Setting the Standard for Country Analysis and Forecasting', http://a330.g.akamai.net/7/330/25828/20051026163306/graphics.eiu.com/files/ad_pdfs/2005Methodology.pdf , 14 July 2008

cover and they take diplomatic roles. There are also intelligence officers under no official cover who pretend to be journalists, businessmen etc. The HUMINT also needs its 'sources' in other countries which can provide with information the intelligence officers. Finally, there are also defectors who betray their governments by providing valuable information to foreign agents.[46]

Regarding the technical sources, imaging reconnaissance capabilities taken by planes were vital for the observation of opponent's plans mostly in the past and in war periods. Currently, the use of satellites becomes more and more extended and modern satellites which can provide even half meter resolution are available to states. Consequently, spy satellites owned by states do not make necessarily a huge difference anymore. Nevertheless, signals intelligence remains a very important area for the success of secret services. Interception of communications as well as of military equipment like radars may prove substantial for the collection of information.[47]

It can clearly be concluded that there is a difference of methods between OSINT analysts and HUMINT, IMINT and SIGINT analysts. It is certain that both are important in the intelligence process. Definitely, however, OSINT products by government-bound intelligence organizations and commercial sector can have a vital contribution in plenty of areas and for a great number of actors. Their applications remain to be analyzed in the next chapter.

[46] Schulsky & Schmitt (2002), pp.11-22
[47] Ibid, pp.22-33

3. Users of OSINT and its applications

OSINT can be a useful tool for a range of different users. In this chapter it will be examined who can make use of OSINT. Firstly, OSINT's applications for governments and especially for the departments of defence will be made clear. Secondly, the utility of OSINT in the operation of international organizations like NATO, UN and NGOs will be explored. Thirdly, I will also try to seek the correlation that NGOs and IGOs have with OSINT. Fourthly, an attempt will be made to understand the contribution of OSINT in business life. Finally, the exploitation of the advantages of open sources by non-state actors with notorious purposes will also be examined.

Applications of OSINT by governments

OSC and BBC Monitoring were mentioned above as producers of OSINT. Although their products are directed mainly to specific national governments, we should take into account all possible OSINT producers that can benefit governments. In general, as Avital Johanan from Jane's argued, OSINT offer governments what they cannot get from their close networks and they have the capability of choosing what they need from the variety of products available.[48] This indicates that OSINT has opened a new window to government agencies and departments since they can fill the gaps that emerge in their analyses by including the added value of open sources.

According to the Jane's analyst, intelligence from open sources can help at avoiding one common phenomenon of the intelligence process. This is the group-thinking.[49] Organizations like Jane's can offer independent analysis and products to intelligence services. As a result, intelligence officials cannot ignore other opinions but they should include them in the all-source analysis they do.

Another advantage that policy makers can take from OSINT products is the stimulation of public's interest and support regarding decisions on issues of foreign and defence policies. When the policy makers share these products with both

[48] Interview at Jane's
[49] Interview at Jane's

domestic and foreign publics they are then able to gain their understanding.[50] For example, by communicating publicly the opponent's intentions for a future illegal military action to the domestic press or to the counterpart's side, policy makers will not only avoid future constraints but they will also raise the local understanding; this would have a positive effect on their plans.

Broadcasting services are also important to governments since real-time translations of foreign radio or television emissions as well as the monitoring of what is written in foreign newspapers on a daily basis can keep government officials and others updated about trends, developments, aspirations or domestic problems. One illustrating example about the value that foreign media analysis can have is given by the case of North Korea. The fact that this country is a closed society makes it even easier to track the plans and priorities of the government since there are only two newspapers, one that belongs to government and one to the communist party.[51] This would not be the same for a democratic country with numerous broadcasting services but still the importance of media should not be neglected since one can always find golden nuggets if he has the adequate structures to look what media serve to their people in other countries.

Furthermore, the contribution of intelligence flowing from open sources can be essential for the departments of defence; in terms of a military level. According to Steele and Lowenthal, this can occur when either a crisis emerges or during a military operation that has already started. More specifically, when a crisis bursts somewhere in the world, policy-makers and commanders need some intelligence to develop their plans on how to react. Open sources like journalists on the ground, foreign media, experts, maps and satellite imagery can have a critical value. Consequently, policy makers can quickly acquire information about the causes and the history of the crisis, any crucial parameters relating to it or the intentions of the sides. Meanwhile the military commanders can get intelligence about the counterparts' capabilities or logistic assessments. [52]

[50] Steele (1998) ,pp.148-150
[51] Burke (2007), p.13
[52] Steele & Lowenthal (1998b)

Furthermore, OSINT would be a necessary asset even in an ongoing operation. This is why commanders need continuously to know the battle order or how the crisis develops in order to make their contingency planning. Commercial satellite imagery and local media could prove very useful in doing so. Moreover, policy makers could get reports and forecasts by experts on the ground or local media broadcasts which can also contribute to further awareness.[53]

Normally, when a country knows its enemies, it is prepared to confront any incidents and it may seem that OSINT is not necessary. However, nowadays, states which participate in alliances have to confront incidents in Third World countries some found in Africa or Asia. It is very hard, even for the most powerful states, to keep an eye in remote regions. Consequently, the planning of an operation or any humanitarian assistance in such an area, where there was no focus from intelligence agencies before, could be very hard.[54] Recent examples that have proven the need for OSINT are the turmoil in Burma and the Zimbabwe crisis.

Another area where OSINT is useful is in counterterrorism planning. Governments can exploit their sources to keep themselves updated about terrorist plans and capabilities. The recently created Department of Defence and Homeland Security in US in particular and similar departments in other countries which are both intelligence and law enforcement agencies make wide use of open sources. Clandestine capabilities have geographical and budgetary limits and, thus, cooperation with local entities in other countries and the use of all the spectrum of open sources can help countries at their early warning system, crisis management and their confrontation of terrorism.[55]

Applications of OSINT by International Organizations

Some of the contingencies that were mentioned above like the crises around the world or terrorism may need to be confronted by international organizations such as NATO and the UN. Many advantages that OSINT provides to single states can also be offered to alliances, even in a greater scale. Furthermore, non-government

[53] Ibid.
[54] Steele (1995a), p.458
[55] Best & Cumming (2007), p.16

organizations also have an increasing role providing their services when a humanitarian crisis emerges due to an outbreak of war or a natural disaster.

Starting from NATO, OSINT can act as a keystone for the planning and execution of a wide range of different coalition operations like peacekeeping and peace enforcement. In coalition operations where many states participate, OSINT has an exceptional value for civil-military collaboration because it is the one that can be shared without fear of disclosing sources and methods used for the acquisition of classified information. Its contribution for the common understanding of the area of operations among all participants, from the alliance forces, other non-NATO nations' forces and various NGOs, is vital.[56]

However, OSINT is even more useful for the out of the area operations due to the nature of needs such as humanitarian assistance and disaster relief that the emerging threats impose. Besides, OSINT is essential because in these operations a huge variety of information is needed about infrastructure, population distribution, local resources or other particularities.[57] Here OSINT helps at the cooperation between NATO and NGOs. NGOs are increasingly active in regions where crises burst by offering food, medicine and shelter. They are important contributors to peace and relief. As a consequence, NATO needs to adapt to their existence and OSINT can help at this symbiosis by coordinating their actions in the area of operations.[58] In addition, NGOs can have an additional value in multilateral operations like those of NATO since they usually have deeper local knowledge and experts on the field comparing to other intergovernmental organizations. An indicative example could be the presence of missionaries of a Church NGO in a conflict area in an African country because they could provide real-time information about the situation on-ground.[59]

This is the new trend that emerges where a bottom-up, multicultural and consensus approach is needed. OSINT can bring all actors together. Government agencies, business communities, NGOs, local communities and everything that each one of

[56] NATO OSINT Handbook (2001), pp.1-3
[57] Ibid, p.3
[58] Ibid, p.33
[59] Koenig (2005)

them can offer should be included in the alleviation of the crises and the improvement of the on-ground situation in every case.[60]

To conclude on NATO and OSINT, in the area of commercial satellite imagery, the benefits for NATO are great since there is no need for exploitation of national spy satellites that only some member-states hold. The only constraints that NATO has in this process of imagery distribution are the copyright ones. All of the countries that participate in the alliance and even those that do not, can share the remote sensing images in hand and can organize better their mission plans, mapping of areas and infrastructure information[61].

Similarly to NATO, OSINT is also an important factor for the realization of the United Nations' responsibilities. UN and NATO exploitation of OSINT resembles because of their quite similar nature. Cooperation between UN and NGOs is frequent in order to facilitate relief and other operations. In addition, satellite imagery as a source of OSINT can offer some more services like detecting compliance in sanctions or detecting atrocities, as it happened in Rwanda, Bosnia, and Kosovo.[62] Moreover, IAEA could use it to monitor if nuclear states abide by the rules and do not violate international arms control agreements. OSINT can also prove helpful in timely responding to refugee movements and managing disputes before an escalation takes place and serious conflicts arise. Another tangible example of satellite imagery utility is the UN efforts to tackle drug trafficking and production by relying on those images.[63] It is unambiguous that commercial satellites and the other open sources are valuable for international organizations. However, it is also useful to know how this intelligence flows among the organizations, governments and NGOs.

Correlation of NGOs and IGOs with OSINT

Apart from direct purchasing of OSINT from private producers or governmental providers, the flow of OSINT takes place mainly through exchanges among its users. On one hand, NGOs with expertise on certain levels, such as humanitarian, human

[60] Burke (2007), p.22
[61] NATO OSINT Handbook (2001), pp.10-11
[62] Boatner (2000), pp.84 & 86
[63] Dehganzada & Florini (2000), p.1

rights or conflict resolution, are capable of producing OSINT that would be mostly welcome by governmental organizations or states. On the other hand, there are governmental organizations like NATO and UN. According to NATO OSINT Handbook, NATO collaborates with NGOs and they can share this OSINT or it can also produce its own using internal resources.[64] In the case of UN, there are many ways of circulating and producing OSINT and they will be analysed below.

As far as external sources are concerned, UN receives reports from agencies like the IAEA and special commissions while NGOs and policy experts are providers of informal and voluntary briefings as well. But there are also many ways of exploiting open sources products which are being developed or collected by internal structures. Especially dedicated departments and fact-finding missions can provide information to the UN which will direct the organisation to its decision making. The Policy Planning Unit and the Early Warning and Contingency Planning Unit are some, among others, of the teams supporting this effort.[65] Another indicator of OSINT sharing is the ReliefWeb which is an information portal administered by the UN Office for the Coordination of Humanitarian Affairs. It operates as a hub of information circulation during humanitarian crises. Information such as maps and documents from UN, governments, NGOs or academia are available there in order to assist the international community confronting timely outbreaks of violence with worrying humanitarian consequences.[66]

Application of OSINT by businesses

OSINT finds plenty of applications in another area. This is the area of businesses where law firms, commercial organisations, financial institutions and others can benefit from OSINT substantially. The OSINT that private providers produce can contribute to the successful performance of all those entities covering a broad spectrum of their needs.

[64] NATO OSINT Handbook (2001), p.vi
[65] Ekpe (2007), pp. 379-387
[66] 'About ReliefWeb',
http://www.reliefweb.int/rw/hlp.nsf/db900ByKey/AboutReliefWeb?OpenDocument , 9 June 2008

Thanks to OSINT forecasting, its users can avoid taking risks that could end up as failures and they can adjust their decision-making in more promising investments and decisions. For example, these forecasts could concern the solvency and the reputation of future partners or the suitability of an environment where a business was going to expand its enterprise. Clients can also mitigate risks because of timely threat assessments that OSINT can yield and they will also be ready to deal with any possible threats. For instance, a region which is prone to terrorist attacks could dissuade an investor from doing more business there. Furthermore, industry trends could provide an early and adequate warning about the chances of success or risks of business operations and this could advice clients to adjust their further decisions accordingly.[67]

Some more specific examples for business applications could be given relying on open sources. Avital Johanan from Jane's claims that OSINT is very useful for companies in the defence industry since they can identify commercial opportunities, needs for future procurement by states and track their competitors' activities in the area.[68] Consequently, they can define their policies and focus their planning according to competitors' or country-based OSINT available. OSINT from imagery can have a great contribution as well. Oil companies can spot locations where oil reserves can be found and mining companies can inspect the surface of areas they want to undertake action.[69] That makes evident that the whole business sector can find great utility in OSINT and can exploit it through many ways.

Applications of OSINT by non-state actors

However, this exploitation knows no limits. Non-state actors cannot be denied the use of open sources since they are available to anyone who has the capabilities to access them. Terrorists can acquire capabilities that governments and intelligence services cannot easily measure. As a consequence they can strike and cause severe pain and fear diminishing the states' ability to protect their citizens.[70] Open sources like the

[67] I used the site of a corporate investigative and risk mitigation company (quest.co.uk) to get some useful insight for this analysis.
[68] Interview at Jane's
[69] Dehganzada & Florini (2000), p.12
[70] Waltz (2003), p.48

Internet, satellite imagery and media can facilitate the preparations of terrorists to inflict turmoil.

Commercial remote sensing is maybe the most important open source for terrorists because it has various applications. Terrorists can be aware of counterterrorist plans and military operations by observing their adversary's actions on ground. Consequently, they can also try to adopt ways to avoid being surprised but compromise opponent's plans. Furthermore, satellite imagery facilitates their plans and terrorist attacks.[71] The examples of the use of Google Earth mapping services by Palestinian terrorists and Iraqi terrorists, who targeted military sites of Israelis and British army respectively, are indicative and worrying.[72] As a result, it can be concluded that commercial satellite imagery offers to terrorists not only the ability to identify and analyse their targets but also to prepare them in the best possible way before they take action.

In addition, Internet is another useful open source in hands of terrorists. First, they can improve their communication and coordination which is a necessary element for a terrorist attack.[73] Similarly to satellite imagery, Internet and media can be used by terrorists in order to collect information for the striking of their targets and recognize vulnerabilities of the target or specific details about it. Furthermore, online information about the construction of bombs could be released by third parties or even accidently by governments. Nevertheless, although the technological innovations and the availability of information from open sources give an advantage to non-state actors, it is not so easy for them to bring their plans in completion if there are no experienced users to handle all these assets.[74] In any case, the beneficial consequences of open sources for terrorists mean that governments' interests, businesses' interests and international organizations activities are in danger and all sides should remain vigilant.

[71] Rowberg (2002), pp.13-14
[72] 'Terrorrockets.com-Google a weapon vs Israel', http://www.nypost.com/seven/10262007/news/worldnews/terrorrockerts_com.htm, 25 May 2008
[73] Jordan, Torres & Horsburgh (2004), p.32
[74] Don, Frelinger, Gerwehr, Landree, Jackson (2007), pp.26-29

It has become obvious above that OSINT has multiple applications. If exploited smartly, it can provide very useful services to governments, various types of organizations and businesses. However, non-state actors can also benefit from OSINT advantages. Analyzing further all possible benefits and weaknesses that OSINT has, we will be in better position to judge its utility for all those users.

4. The benefits and weaknesses of OSINT

After having presented the various trends in OSINT applications, the utility of OSINT will become more evident by demonstrating the benefits open sources provide. Among the advantages, it is also worth mentioning how OSINT contributes to the all-source intelligence process by supplementing clandestine sources. Nevertheless, the drawbacks of open sources will also be examined so that an overall image is acquired about the role of OSINT.

Benefits of OSINT

By bearing in mind the OSINT applications, some features and advantages could be understood more easily. First of all, the speed with which open source information is collected and turned into actionable intelligence is a great advantage for possible users. This is essential since the existence of clandestine assets in remote and other non high-risk areas is not only uncommon but also impossible to happen.[75] However, a call on open sources can give some real time responses for the intelligence needs. Therefore, the speed provides timeliness and it is a valuable asset in hands of users such as policy makers and military commanders.

There is also the issue of quantity as long as there are plenty of open sources that can be used as information providers. OSINT analysts compile all this data input and could transcend or match the effectiveness that a smaller number of case officers, based on clandestine sources, could have.[76] As a result, using OSINT, the coverage of an issue can take place from many different perspectives and this is positive because an overall assessment of the situation will be the final contribution.

[75] Mercado (2005)
[76] Mercado (2005).

The issue of quantity could push us further to seek also the answers about the quality of OSINT. Quality is difficult to be measured before the intelligence product is put into practice and the end-users are the ones to assess OSINT quality. However, OSINT accountability and reliability are two useful means which can indicate its quality. On one hand, policy makers rarely have the chance to know the sources that provided traditional intelligence to them because of the need to keep secure these sources and methods. Policy makers do not have the opportunity to access the raw data and, consequently, they have to rely on final products. On the other hand, reports on OSINT can provide sources, data and the route of the intelligence processing to their receivers. The OSINT process can direct its analysis to clients' needs and, thus, OSINT gain their trust for its ability to satisfy their demands.[77]

Furthermore, the nature of OSINT facilitates the ease of its use among the intelligence officers, analysts and users. The absence of the classification necessity enables the exploitation of information at all levels.[78] Therefore, OSINT, which has no flow restrictions, can contribute in building trust due to its sharable character and capacity to enable better communication among partners. In this way, as it was examined in the previous chapter, it facilitates the cooperation between international organizations or governments.[79] And since in the intelligence world the ability to share is a real rare phenomenon, it makes sense why this attribute of OSINT is one that makes it special.

Another real important advantage for OSINT is its cost. The majority of open sources do not necessitate great costs to be exploited. Sources like media, bloggers, experts on the ground or Google-earth services are quite inexpensive if we consider what governments spend for their clandestine activities. Especially for small and medium-sized states, OSINT offers a really added value to their intelligence agencies.[80] In addition, what makes OSINT less costly is also the fact that the expertise for the exploitation of open sources does not necessarily need to come from public services and structures, since the private sector can be a great provider.[81] For example, states

[77] Burke (2007), pp.11-12
[78] Mercado (2005)
[79] Gibson (2004), p.20
[80] Pallaris (2008) ,p.2
[81] Steele (2002), p.71

do not need to build their own intelligence satellites if they use commercial satellite imagery.

What is more, there is no political risk in OSINT acquisition.[82] Since it relies on ethical and legal collection from publicly open sources, the states could not be blamed for illegal ways of information collection. This is an additional benefit that could motivate governments into using it.

Contribution to clandestine capabilities

Apart from the general benefits of OSINT analysed above, OSINT can also have a non-negligible contribution to clandestine collection capabilities. Firstly, open sources like media, blogs and news agencies can work as providers of 'tip-off' for probable threats and emergencies. Tip-offs could offer an insight to governments or organizations about the intentions of opponents or the development of new military warfare. [83] As a result, this could enhance the preparedness and the allocation of priorities by clandestine facilities.

Secondly, the existence of the OSINT capability can free classified assets which are sacrificed for the acquisition of information that is available openly. As a consequence, open sources can be optimized for some specific intelligence problems and classified sources can target where the situation necessitates their use. Furthermore products developed using clandestine ways can validate OSINT ones.[84] After which, an OSINT validated product would become more acceptable by end-users. What could finally be said about this relationship between clandestine and OSINT collection methods is depicted very simply in the following statement: 'You don't send a spy where a schoolboy can go'.[85]

Thirdly, OSINT can be used as a context for further classified activities. As Joseph Nye says: 'Intelligence problem is like a jigsaw puzzle, with open sources providing

[82] Ibid, p.65
[83] Bowen (1999), p.51
[84] NATO OSINT Handbook (2001), p.40
[85] Steele & Lowenthal (1998a), p.46

the outer edge pieces, without which one can neither begin nor complete the puzzle'.[86] This indicates that OSINT is able to have a proactive character setting the background and directing the clandestine sources to focus where there is need. An example could be the situation when spy imagery spots a ship but OSINT is adept to say what the cargo of that ship is according to the port the ship loads or where is it going according to its itinerary.[87]

Fourthly and finally, the fact that OSINT can cover and protect the existence of classified sources and methods is crucial. Governments can present open sources as the ones that were used to collect their information or collaborate with others in international organizations by sharing it.[88] Keeping this trend of utilizing the advantages of OSINT, clandestine methods and sources can really benefit and be more effective.

Weaknesses of OSINT

Despite the benefits which illustrate OSINT's great value, one should also recognize some weaknesses when dealing with its applications and utility. The most notable one is the information overload that could result when the collection from open sources takes place. Sometimes, the level of noise is very high and time-consuming efforts should be made in order to extract the golden nuggets and provide them to the end-user.[89] The available information can be too much or contradictory and the analysts have to analyse meticulously the open sources to find what they seek. Sometimes they may not be enough in numbers to cope with it. For instance, media and Internet are two sources that make available a big bulk of information that is confusing for the collection and analytical processes.

Furthermore, it is hard to verify the accuracy of open sources information. The analyst could be deceived by inaccurate, irrelevant or non validated information. Especially in media which are fundamental sources of OSINT, it is not easy to discern disinformation techniques. Sometimes, media or web portals are under control of governments or businessmen and their information is impartial or biased.

[86] Steele (1995b), p.222
[87] NATO OSINT Handbook (2001), p.40
[88] Ibid, pp.40-41
[89] Pallaris (2008), p.2

Consequently, it rests upon the analysts themselves to critically judge which source is beneficial for their purposes and which one provides misleading information.[90]

An additional issue is this of language and translation since a substantial number of open sources are available only in foreign languages.[91] OSINT operates in an international spectrum and the need for personnel capable of translating open sources is explicit. This is a serious barrier that national intelligence agencies confront and they often rely upon private sector for those services.

The former issue of language raised the need for the staff expertise and coordination. Since OSINT is in each early stages of real status recognition by the intelligence community, it happens to suffer from a lack of specialized experts and networking. The duplication of efforts should be avoided for reasons of cost and effectiveness. And, moreover, the exchange of viewpoints and resources should be facilitated by adequate structures so that the best possible results from OSINT will be realized.[92]

Another issue to grasp our attention is that the Internet can prove to be a two-edge sword. When governments share information online with friends they may leave trails which will point out their intentions. If this happens, security of networks may be compromised and the beneficial aspect of the Internet can turn hostile very easily. Therefore, the exchanges between every kind of actors should take place under careful disguise because leaking can prove detrimental.[93]

Last but not least, except for the weaknesses which depend on the open sources nature and use, there is another limitation which affects unfavourably the OSINT. It is an intrinsic problem to deal with and this is the cultural bias for classified sources as a sufficient intelligence provider. Many intelligence analysts or officers are negatively prejudiced about the exploitation of open sources and they search for answers in classified ones although these sources have narrower perspective.[94] They assess the level of importance for the intelligence accordingly to the means used to extract it or

[90] Hulnick (2002), pp.567-568
[91] Studeman (2002), p.57
[92] George (1998)
[93] Burke (2007), p.14
[94] Holden-Rhodes (1997), p.15

its secrecy. However, it seems that gradually the intelligence community appreciates more the benefits of open sources. The creation of OSC in the United States is one promising example.

To conclude on the benefits and the weaknesses of OSINT, it could be argued that the advantages seem to outnumber the drawbacks. All the benefits of OSINT could prove substantial for the evolution of the all-source intelligence process and OSINT seems to have great capabilities to offer. However, the weaknesses should not be underestimated. Most of them occur because of the new role that OSINT has acquired recently. If the intelligence community casts more attention on OSINT potential, then, problems like the barrier of language, the deception because of disinformation, careless leaking or even the information overload could be dealt and reduced sufficiently. What it takes to find solutions and improve OSINT as a discipline can be spotted more on the willingness of the intelligence community to change its former attitude towards OSINT and give it the respect and credit for what it can do. Therefore, if the right choices are made in various levels, like the personnel training and the allocation of sources, the OSINT benefits will enrich the all-source intelligence products.

5. The private sector and its contribution to the OSINT

The general benefits and limitations of OSINT helped us understand further its value and I will now try to focus on some of the private sector capabilities and features which should be taken into account when dealing with the OSINT. By examining comparatively the private sector companies and the government agencies, we could discern their strengths and weaknesses. But, mostly, their supplementary nature and positive influence for government clients will become evident. Examples about how government-bound intelligence organizations exploit private companies are cited at the end of this chapter.

Comparison between private sector and government departments

Nowadays, OSINT has an increasing importance for commercial clients and it becomes a fundamental tool for them since it can provide actionable competitive

intelligence and help in the decision-making due to all the advantages mentioned earlier. That means that on a governmental level, especially in defence and security, action should also be taken by governments in order to exploit the advantages of private OSINT and complement the public capabilities.[95]

First of all, the private sector possesses more and relatively better technological means to collect information and turn it into OSINT. The fact that the private companies have already developed the infrastructure that is needed for OSINT facilitates the government agencies to exploit what is already available.[96] One notable example is the suppliers of high resolution satellite capabilities. The increasing number of suppliers leads to less expensive, more competitive, and thus, more trustworthy products. [97] Another example is the Intelink-U. This is a virtual private network which provides a secure environment, a government intranet where open source information can flow from intelligence agencies to other organizations. The Intelink-U is operated by a private company and it enables the distribution of unclassified material.[98] Those examples indicate that the private sector has the necessary tools, techniques and specialized staff. Consequently, OSINT's effectiveness depends on the exploitation of private sector's expertise and its state-of-the art technologies.[99]

An issue that is often raised about the capabilities of the OSINT on the government level concerns the size of the intelligence services budget which is allocated to that level. It is known that the lion's share of the intelligence budget is devoted to the clandestine discipline as well as that there is a general tendency of reduction in defence budgets. However, the needs of OSINT are expanding continuously; the exploitation, therefore, of private resources becomes a necessity. This imported experience should be supplemented with the organic knowledge coming from inner sources.[100] According to Robert Steele, the private sector can help the government/intelligence community live up to the expectations that the modern world

[95] Gibson (2004), p.20
[96] Quiggin (2006)
[97] Rathmell (2002), pp.75-77
[98] 'Intelink-U', http://fmso.leavenworth.army.mil/wbil/osisinfo.htm , 20 August 2008
[99] Rathmell (2002), pp.75-77
[100] Wilby (1998), p.6

raises since there is still lack of training, capabilities and organization in the intelligence agencies.[101]

Private intelligence companies can contribute substantially to the intelligence agencies' efficiency and this becomes obvious easily. Apart from the weak areas mentioned about the capabilities of the international community, another characteristic of OSINT government departments is that their analyses are usually biased by ideological preferences and policy directives. As a result, they have a narrower mindset when dealing with certain issues.[102] For instance, a government may get involved in a crisis in order to get political or other strategic returns in its aftermath. In this case, OSINT analysts may focus only on what would encourage this engagement instead of casting emphasis on possible negative signals in present or in future. On the other hand, private sector companies who conduct open source research can provide a more independent product. They have no preoccupied beliefs about the fields of their analysis and this contributes to the quality and usefulness of their product.

Furthermore, private companies focus their assessments mainly on long-term trends such as possible emergencies in different remote regions. In contrast, on a governmental level, the support of certain policies requires actions of relatively shorter-term trends. [103] Nevertheless, we cannot claim that there are strict boundaries about the areas and the effectiveness in each sector of research, both private and public. What can be extracted from this is that the harmonized cooperation of both sectors can bring the most useful results for the sake of governments.

In addition, OSINT produced by private vendors has the advantage to provide tailored products to a wide variety of clients. In the interest of serving of customers' needs, they create private databases and other ad hoc projects or develop software.[104] Therefore, the private sector serves simultaneously a big number of different clients. These companies have both the sources and well-trained personnel in order to respond to various issues, in various different locations. This comes in contrast with the

[101] Steele (1995), p. 218
[102] Harris (2005)
[103] Ibid
[104] McGill (1994), p.439

government agencies which have not the same potential either in the variety of targets or in depth of analysis. Nevertheless, as Avital Johanan form Jane's noted, the tailored product to governments is not always very easy to be provided. Their intention to avoid disclosure of their plans and targets sometimes makes them prefer more general reports to detailed products from private OSINT organizations.[105]

However, despite the great capabilities of private companies, government officers cannot be replaced. The service of translation could underline this substantial role of intelligence officers. Since the personnel of intelligence services are limited on this service, intelligence community hires contractors to provide translations. On one hand, the specialized staff officers, which provide this service, have one master-recipient and they are logically more focused on a single target. On the other hand, contractors approach every assignment as one among the others. Apart from their unavailability at important moments because of other assignments, they will also not work with the zeal of an intelligence employer.[106] This example does not mean that the private sector acts unprofessionally. Far from it, since their intention is to deliver their best services to plenty of clients and gain profit. The intelligence services, however, have the duty to protect the national interests and their devotion is a sine qua non for the intelligence process.

The issue of cost is another area of comparing private producers of OSINT and government agencies. OSINT, in general, is the relatively cheaper solution and, when it is possible to be applied by the intelligence community, provides a definite advantage for saving valuable resources for other intelligence needs. However, the private OSINT outsourcing can end up as an expensive facility if a specialized contracting process is not established. Various users inside the government agencies should be able to reach the valuable private provisions without additional intermediary and administrative charges.[107] The comparative cost between the use of classified and open sources is vast. But the open sources may prove less useful and more costly if the intelligence community does not have the adequate structures to manage and exploit them.

[105] Interview at Jane's
[106] Mercado (2005)
[107] Hamilton (2007), p.248

Finally, a distinction could be made about OSINT. The OSINT provided by the intelligence agencies can be validated by the clandestine sources and be included in the all-source intelligence product. In contrast, OSINT produced by the private sector cannot be verified in the same way.[108] Despite the fact that governmental classified and technical sources may verify the intelligence given by this sector, the sources used by a private company cannot be that clear. This could cause concern to governments since they need to be aware of the information sources in order to defend their choices. However, because companies are interested in efficiency and timely responses to strict deadlines set by their commercial clients, they do not mind so much for the traceability of their sources.[109] However, this does not undermine the value of OSINT, because private companies focus more on the result than on the whole process. It does not mean that they have vague or illegitimate sources but it is simply a matter of interests. While commercial clients are interested in their success in financial terms, governments do so in national interest terms and their attitude is different on this issue. [110]

Exploitation of private companies by government departments

In their attempt to serve the national interest, governments may at times find it imperative to exploit the services of the private sector. The technical expertise of the private companies is relatively better, their capital is bigger and their services operate in a faster pace than those of government-bound intelligence organizations. There are many ways of exploiting the commercial sector. Firstly, governments may subsidize specific programmes that the private sector would hesitate to develop because of high risk or lack of necessity. As a result, the intelligence services may reap the fruits of this investment as it happened in the cooperation between the Defence Department of US and commercial imagery companies in 1998.[111]

Secondly, governments may offer flexible regulation to companies which want to invest in technology that could threaten governments' interests. For example, if a

[108] Lowenthal (1998)
[109] Hamilton (2007), p.249
[110] Ibid, p.248
[111] Berkowitz & Goodman (2000), pp.51-52

company is able to sell satellite imagery with resolution of one meter, this would probably be against a government's interests. Consequently, a government may buy the high resolution product and agree with the company to provide only images of lower resolution to other users.[112]

Thirdly, in the post-Cold War environment, intelligence agencies are in need of analysts with different expertise on different subjects and locations. Intelligence agencies could find ways to hire these OSINT analysts from private organizations when situations call them to draw on expertise in other more rare issues. [113] These issues are usually located in remote regions where only academic or financial interests exist. Though, it will not be an easy venture since academics or businessmen may be less eager to work for intelligence organizations than for other government agencies[114].

Having emphasized some of the most important elements of the private sector, in general, and of OSINT companies, in particular, the significance of private sector was made clear. Following the standards of private sector, improvement of government agencies will also be realized as long as they are still underdeveloped in the management of open sources. The continuous and further integration of private organizations with intelligence services and their cooperation could result in a beneficial outcome for the sake of intelligence community.

[112] Berkowitz & Goodman (2000), pp.52-53
[113] Ibid, pp.56-57
[114] Schulsky & Schmitt (2002), p.143

6. A new era for OSINT?

So far, the discussion of the advantages and applications of OSINT demonstrates OSINT's utility and potential capabilities for a wide variety of users. The precious nature of OSINT in the beginning of 21st century has become more apparent due to the co-existence of a facilitating environment for the development of the OSINT. Currently, two fundamental features of this international environment are the unpredictable and asymmetric threats that have come to the front after the end of the Cold War and the information revolution along with its consequences.

New international environment and new threats

The intelligence needs of the modern world are different from the ones in the past. During the Cold war era, the western intelligence community had one adversary -the Soviet Union- and one purpose -its containment. Crises taking place around the world could be placed in this Cold War framework, since there were two spheres of influence; the Soviet and the American. There were no new issues and the opponents knew where to focus their attention, namely on the other's capabilities. For example, a typical continuous area of interest was the Soviet strategic missile forces. As a result, the counterparts could organize their intelligence agencies' structures adequately, the personnel were specialized on one single target and there was only an evolution of techniques and problems. No revolution and no surprise could catch any intelligence agency unprepared.[115]

However, the international environment has changed significantly after the demise of the Soviet Union and new threats for the national and international security emerged. Upon closer examination, most of them are not actually new but they just became more evident at the end of 20th century and in the beginning of the 21st. The intelligence system which was used to deal with the large scale threats is adapting to the threats of the new environment. According to George Tenet, the former US Director of Central Intelligence Agency (CIA), these threats include international terrorism, proliferation of weapons of mass destruction and their delivery systems,

[115] Berkowitz & Goodman (2000), pp.3-4

rogue states that threaten the stability of whole regions or other states, information warfare threats against governments and other traditional conflicts in unstable regions of the world.[116]

When dealing with international terrorism, our attention focuses on non-state actors which have proved how catastrophic the consequences of their actions may be, as demonstrated by the attack of 9/11 on the World Trade Center. Terrorists constitute a threat which is hard to identify and to deal with because of the vague structures of their organization, their widespread networks, as well as because of the way they conduct their operations. The established intelligence methods and structures proved unable to prevent the events of 9/11; in general, conventional ways of trying to confront terrorism do not seem to work.[117] Terrorist movements rely essentially on the use of open sources, available mainly on the Internet (about 4000 pro-Al Qaeda web sites and chat rooms), to recruit and provide virtual training, and conduct their operations using encryption techniques.[118]

The proliferation of weapons is another crucial issue; non-conventional weapons, including nuclear, chemical, biological and radiological weapons are a matter of concern as are conventional weapons, some of which dispersed in former satellite states, following the collapse of the Soviet Union. According to one estimate, there are 1.5 million Kalashnikovs in Mozambique alone![119] Furthermore, there is also a proliferation of weapons-building technology and this technology in the possession of wrong hands could have serious consequences.

In addition, crises burst continuously in remote places for various reasons such as ethnic, religious and nationalistic ones. Rogue states under authoritative regimes cause pain to their people or to their neighbours, like the junta in Burma or the situation in Darfur. The international community feels the obligation to intervene but, at times, it proves hard to do so. Intelligence agencies are not so flexible to keep pace with developments in these remote areas or cannot cooperate between themselves and

[116] Waltz (2003), pp.48-49
[117] Dupont (2003), p.34
[118] De Borchgrave, Sanderson & McGaffin (2006), pp.3&13
[119] Berkowitz & Goodman (2000), p.11

other organizations because of anachronistic structures and bureaucratic constraints.[120]

All these examples indicate the importance that OSINT could have in dealing with a multi–threat environment. To start with terrorism activities, before terrorist attacks are carried out, their coordination takes place through open networks while warnings, information about plans, means of attack and potential targets are circulating in open means. Sharing OSINT can be valuable providing fast coordination among officials at all levels without clearances.[121] The lack of this collaboration was given as an excuse about the terrorist attacks of 9/11; reportedly, various pieces of intelligence never made their way to the right officials to take action. By exploiting resources like Internet and the media, intelligence agencies could vitally contribute avoiding terrorist attacks or, at least, prepare to more effectively confront the terrorists. However, despite the importance of OSINT, it cannot provide early warning prior of an attack since the terrorists make sure to keep this stage of their action unknown.[122]

In a similar way, the proliferation of weapons could also be faced by OSINT. For instance, we can take the case that a nation is building a nuclear weapon or missiles of long range. There are lots of scientists and engineers who participate in that nation's weapons-development programmes. Subsequently, certain of its bureaucrats and traders may be included with the possible sale of those weapons to friendly states. The role of OSINT is to track any information that may leak or become available to the public. People like scientists and engineers attend conferences, publish articles, bureaucrats give orders and traders provide future clients with brochures.[123] A recent OSINT success in this area was the U.S. intelligence assessment of Iran which shows that Iran had suspended its nuclear programme in 2003; that assessment was made possible by satellite images of the Natanz nuclear facility.[124] Because critical information is openly available, OSINT analysts should be equipped appropriately to detect it in a timely manner.

---

[120] Rathmell & Valeri (1997), p.524
[121] De Borchgrave, Sanderson & McGaffin (2006), pp.13-21
[122] Tow & Yeo (2005)
[123] Mercado, (2004)
[124] 'Today's spies find secrets in plain sight', http://www.usatoday.com/tech/news/surveillance/2008-03-31-internet-spies_N.htm , 3 June 2008

As far as the emerging crises are concerned, this is an area where OSINT sharing among intelligence services, non-government organizations and international organizations could shape timely and comprehensive responses. Apart from it, in these cases, openly available information could prove very useful since there is normally a clandestine sources vacuum there.

Information revolution

Most of these asymmetric threats developed during the information age which is another reason why the international environment has received such a different character. In general, the information revolution can provide all users with better connectivity, better capabilities and fewer costs.[125]

Non-state actors can benefit from the information technology and they can exploit innovations in telecommunications, computing and miniaturization in order to act faster and more successfully, and with less cost.[126] The communication among terrorists via satellite phones before an attack could be indicative of the application of information technology. In total, non-state actors make use of advanced technology, but it could be argued that this is a dual-use technology, since its proper exploitation could bring very helpful results to both the terrorists and the intelligence agencies.

As far as the software is concerned, the impact has been significant on government intelligence agencies. Without a doubt, electronic dissemination facilitates and accelerates the intelligence process. In the case of OSINT, software has enabled analysts to review the products in a relatively faster way and to have virtual meetings, contributing to improved product accuracy and greater product quality.[127] Software facilitates communication and this helps at spotting faults in data processing and correcting them at any stage.

On OSINT level, information revolution can have a great effect because OSINT effectiveness is intertwined with technological innovations. The developing media

[125] Berkowitz & Goodman (2000), p.13
[126] Ibid, p.8
[127] Sharfman (1995), p.209

services worldwide, the Internet explosion and the continuous evolution in satellite technology render the global societies' exposure wider and open information more ubiquitous. Subsequently, the resources of OSINT multiply in this environment and contribute to the development of this intelligence discipline.

It could also be argued that OSINT is gradually expanding into areas which traditionally belonged to other disciplines. Commercial satellite imagery supplements IMINT and media or networks of experts provide partly what HUMINT provides. Nevertheless, OSINT cannot replace classified intelligence totally. Intractable problems necessitate classified collection and services such as the NGA (National Geospatial-Intelligence Agency) and clandestine reporting will always have a critical role.[128]

Undoubtedly, the new world order and the information revolution have changed the status quo of the modern world. Intelligence agencies should adapt to these changes. Non-state actors try to exploit the advantages of this open source environment. States, along with international organizations, should do so more successfully. The contribution of commercial sector companies is vital in this effort; the era in which OSINT will be a sine qua non for the intelligence community is approaching.

[128] Mercado (2004)

Conclusion

After this thorough examination of the OSINT nature, its producers, its applications, its benefits and its compatibility with the international environment, we can set forth some conclusions and some proposals about what should be done. These deductions may demonstrate my personal viewpoint about the OSINT discipline but I think that they are justifiable and objective after this analysis.

As far as the conclusions are concerned, we could claim that sources like the Internet, the electronic media and the satellite imagery have arisen as vital suppliers of information. Collection of this information and its further elaboration could result in actionable and timely OSINT intelligence. Furthermore, the establishment of OSC in US in 2005 as well as the eminent role of private companies indicate the significance that OSINT has recently acquired. The whole series of assessments and analyses they produce like threat assessments, country profiles, economic and political forecasts can prove extremely important to decision-making for governments, international organizations or businesses. On the other hand, similar to any other dual use technology, open sources can benefit also actors like terrorists and therefore the intelligence community should pay attention to any vulnerabilities that the use of open sources may have. Regarding the private companies, intelligence community ought to exploit all the advantages that these companies provide such as high technology, unbiased analysis and fewer costs. If government departments manage to integrate all these capabilities, then they will be able to reap all the subsequent benefits.

Apart from the numerous advantages that OSINT can provide, there are some weaknesses which should be taken into account. In my opinion, none of them is insurmountable. If OSINT receives the attention it merits from the intelligence community, it can surpass all the possible barriers. The most substantial is the information overload. This is a real problem in an open world which produces myriads of information. With adequate expertise, however, and with exploitation of technology innovations and private sector's capabilities, this information can be more controllable.[129] Moreover, the cultural bias for classified sources should cease to exist.

[129] Stephen Mercado (2007), Vol48.3

It is difficult for the intelligence community's culture to change but this is a vital prerequisite if the OSINT is expected to reach all its potential. This culture could initially change by the redistribution of the budget and the allocation of more economic resources and respect to OSINT. Furthermore, this could happen by employing more officers competent in languages like Chinese, Farsi and Arabic and by employing more staff capable to cope with open sources collection and analysis.[130] Therefore, it can be concluded that it is a matter of willingness and adaptation. If intelligence community manages to deal with it, then it could render the OSINT fully equipped to meet the challenges of the modern world.

These challenges that started arousing after the end of Cold War benefited from the information revolution in recent years. We live in a world of openness and governments should be able to adapt to this environment and run their agencies according to the emerging needs and challenges. The OSINT discipline seems to be adequately-suited to deal with them since it has the tools and the status to handle these difficult circumstances.

To conclude, I strongly believe that Open Source Intelligence can acquire a dynamic role in the intelligence process of the 21st century. Clandestine intelligence disciplines will always be necessary and cannot and should not be ruled out. OSINT can supplement them and fill in the gaps that exist. In a modern environment, intelligence community should come up with an answer. In my opinion, it seems that OSINT is the best possible answer. If its potential capabilities attract the proper attention by governments, intelligence agencies and other government, non-government and private organizations, then the indispensable role of OSINT will become more evident than ever. OSINT has just appeared on the stage and it is going to stay there for long.

[130] Ibid

Bibliography

Books

1) Berkowitz Bruce & Goodman Allan (2000), *Best Truth: Intelligence in the Information Age,* (Yale University Press/New Haven and London)

2) Holden Rhodes J.F (1997), *Sharing the Secrets: Open Source Intelligence and the War on Drugs,* (West Port-USA: Praeger Publishers)

3) NATO (2001), *Open Source Intelligence Handbook,* http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf , 25 May 2008

4) NATO (2002), *Intelligence Exploitation of the Internet,* http://www.oss.net/dynamaster/file_archive/030201/1c0160cde7302e1c718edb08884ca7d7/Intelligence%20Exploitation%20of%20the%20Internet%20FINAL%2018NOV02.pdf , 25 May 2008

5) Shulsky Abram & Schmitt Gary (2002), *Silent Warfare: Understanding the World of Intelligence,* 3rd edn. (United States: Potomac Books)

6) Steele Robert (1998), 'Information peacekeeping: The Purest form of War', in Matthews Lloyd, ed. *Challenging the United States Symmetrically and Asymmetrically: Can America be defeated?* , (Pennsylvania: DIANE Publishing), pp.143-172

7) Steele Robert & Lowenthal Marc (1998a), '*Open Source Intelligence: Executive Overview'*, OSS Academy, http://www.earth-intelligence.net/dynamaster/file_archive/040319/1a981c50936bdaa7a8aaf8fb1ad698a0/OSS1999-E2-11.pdf , 10 June 2008

8) Waltz Edward (2003), *Knowledge Management in the Intelligence Enterprise* (London-Boston: Artech House)

Articles

1) Boatner Helene (2000), 'Sharing and using intelligence in International Organizations: Some Guidelines', *National Security and Future,* Vol1, No.1, pp.81-92, http://hrcak.srce.hr/file/28761

2) Bowen Wyn (1999), 'Open-Source Intel: A Valuable National Security Resource', *Jane's Intelligence Review*, November 1999, pp.50-54

3) Dupont Alan (2003), 'Intelligence for the Twenty First Century', *Intelligence and National Security,* Vol.18, No.4, pp.15-39

4) Ekpe Bassey (2007), 'The Intelligence Assets of the United Nations: Sources, Methods and Implications', *International Journal of Intelligence and Counterintelligence,* Vol.20, No.3, pp.377-400

5) Gibson Stevyn (2004), 'Open Source Intelligence: An Intelligence Lifeline', *The RUSI Journal*, Vol.149, No.1, pp.16-22, http://www.informaworld.com/smpp/title~content=t777285713 , 28 June 2008

6) Hamilton Bean (2007), 'The DNI's Open Source Center: An Organizational Communication Perspective', *International Journal of Intelligence and Counterintelligence,* Vol.20, No.2, pp.240-257

7) Harris Shane (2005), 'Intelligence Shop', *Government Executive*, Vol.37, No.7, http://www.govexec.com/features/0505-01/0505-01na3.htm , 15 August 2008

8) Hulnick Arthur (2002), 'The Downside of Open Source Intelligence', *International Journal of Intelligence and Counterintelligence*, Vol.15, No.4, pp. 565-579

9) Jorda Javier, Torres Manuel & Horsburgh Nicola(2004), 'The Intelligence Services' Struggle Against al-Qaeda Propaganda', *International Journal of Intelligence and Counterintelligence,* Vol.18, No.1, pp.31-49

10) Koenig Carol (2005), 'Non-governmental and International Organizations', *Military Intelligence Professional Bulletin,* http://findarticles.com/p/articles/mi_m0IBS/is_4_31/ai_n16419810 , 5 July 2008

11) McGill Mert (1994), 'OSCINT and the Private Information Sector', *International Journal of Intelligence and Counterintelligence*, Vol7, No.4, pp.435-443

12) Mercado Stephen (2004), 'Sailing the Sea of OSINT in the Information Age: A venerable Source in a New Era', *CIA, CSI Publications, Studies in Intelligence.* Vol.48, No.3, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no3/article05.html , 15 July 2008

13) Mercado Stephen (2005), 'Reexamining the Distinction between Open Information and Secrets', *CIA, CSI Publications, Studies in Intelligence.* Vol.49, No.2, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/Vol49no2/reexamining_the_distinction_3.htm , 15 April 2008

14) Pallaris Chris (2008), 'Open Source Intelligence: A Strategic Enabler of National Security', *Center for Security Studies (CSS) Analyses in Security Policy*, Vol.3, No.32, pp.1-3, http://www.isn.ethz.ch/pubs/ph/details.cfm?lng=en&id=50169, 29 June 2008

15) Rathmell Andrew (2002), 'The Privatization of Intelligence: A Way Forward for European Intelligence Cooperation-Towards European Intelligence Policy', in *NATO Open Source Intelligence Reader*, pp.74-79,

http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/NATO%20OSINT%20Reader%20FINAL%2011OCT02.pdf , 15 November 2007

16) Rathmell Andrew & Valeri Lorenzo (1997), 'Implementing Open Source Intelligence', *Jane's Intelligence Review*, November 2007, pp.523-525

17) Rotheray Brian (2002), 'New Risks of Crisis-Fresh Perspectives from Open Source', in *NATO Open Source Intelligence Reader,* pp.35-38, http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/NATO%20OSINT%20Reader%20FINAL%2011OCT02.pdf , 15 November 2007

18) Sharfman Peter (1995), 'Intelligence Analysis in an Age of Electronic Dissemination', *Intelligence and National Security*, Vol. 10, No. 4, pp. 201-212

19) Soule Mason & Ryan Paul (2002), 'Gray Literature', in *NATO Open Source Intelligence reader*, pp. 25-30, http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/NATO%20OSINT%20Reader%20FINAL%2011OCT02.pdf, 15 November 2007

20) Steele Robert (1995a), 'The Importance of OSINT to the Military', *International Journal of Intelligence and Counterintelligence*, Vol.8, No.4, pp.457-470

21) Steele Robert (1995b), 'Private Enterprise Intelligence: Its potential Contribution to National Security', *Intelligence and National Security*, Vol.10, No.4, pp.212-226

22) Steele Robert (2002) 'Open Source Intelligence: What is it? Why is it Important to the military?', in *NATO Open Source Intelligence Reader*, pp.64-73,

http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/NATO%20OSINT%20Reader%20FINAL%2011OCT02.pdf , 15 November 2007

23) Studeman William (2002), 'Teaching the Giant to Dance: Contradictions and Opportunities in Open Source within the Intelligence Community', in *NATO Open Source Intelligence Reader*, pp.56-63, http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/NATO%20OSINT%20Reader%20FINAL%2011OCT02.pdf , 15 November 2007

24) Tow Jonathan & Yeo Weimeng (2005), 'The Role of Open Source Intelligence in the Global war on Terror', *Institute of Defence and Strategic Studies (IDSS) Commentaries,* http://www.rsis.edu.sg/publications/Perspective/IDSS512005.pdf , 6 July 2008

25) Umphress Lt Col David (2005), 'Diving The Digital Dumpster: The impact Of The Internet On Collecting Open Source Intelligence', *Air And Space Journal*, Vol.19, No.4, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj05/win05/umphress.html , 10 June 2008

Reports

1) Best Jr Richard & Cumming Alfred (2007), 'Open Source Intelligence (OSINT): Issues for Congress', *Congressional research Service (CRS) Report for Congress*, December 2007, http://ftp.fas.org/sgp/crs/intel/RL34270.pdf , 20 June 2008

2) Borchgrave De Arnauld, Sanderson Thomas & McGaffin John (2006), 'Open Source Information: The missing Dimension of Intelligence', *A Report for the Center for Strategic and International Studies (CSIS) Transnational Threats project*, http://www.csis.org/media/csis/pubs/060301-deborchgrave-opensourceinfo.pdf , 14 July 2008

3) Burke Cody (2007), 'Freeing Knowledge, Telling Secrets: Open Source Intelligence and Development' *Centre for East-West Cultural and Economic Studies Research Papers,* http://epublications.bond.edu.au/cgi/viewcontent.cgi?article=1010&context=cewces_papers , 28 May 2008

4) Dehganzada Yahya & Florini Ann (2000), 'Secrets for Sale: How Commercial Satellite Imagery Will Change the World', *Carnegie Endowment Report,* http://ftp.fas.org/sgp/crs/intel/RL34270.pdf , 3 June 2008

5) Director of National Intelligence Open Source Center, Appendix E (2006), in 'Open Source Intelligence', *Field Manual Interim, ,US Department of Army,* http://www.fas.org/irp/doddir/army/fmi2-22-9.pdf , 10 June 2008

6) Don Bruce, Frelinger David, Gerwehr Scott, Landree Eric & Jackson Brian (2007), 'Network Technologies for Networked Terrorists', *Rand Report,* http://www.rand.org/pubs/technical_reports/2007/RAND_TR454.pdf, 13 June 2008

7) Lowenthal Mark (1998), 'Open Source Intelligence: New Myths, New Realities', *Defence Daily Network Special Reports,* http://www.oss.net/dynamaster/file_archive/040319/ca06aacb07e5cb9f25f21babf7ef2bf0/OSS1999-P1-08.pdf , 22 June 2008

8) Rowberg Richard (2002), 'Commercial Remote Sensing by Satellite: Status and Issues', *Congressional research Service (CRS) Report for Congress,* January 2002, www.licensing.noaa.gov/RL31218-RemoteSensing.pdf , 13 Jun 2008

9) Steele Robert & Lowenthal Mark (1998b), 'Open Source Intelligence: Private Sector capabilities to Support DoD Policy, Acquisitions, and Operations',

Defence Daily Network Special Report, http://www.fas.org/irp/eprint/oss980501.htm , 25 May 2008

10) George Patrick (1998), 'The Role of Open Source Intelligence within the Intelligence Process' (1998), *in European Open Source Intelligence Workshop by (EUFIS) in association with International Centre for Security Analysis*

11) Wilby David (1998), 'Open Source Support to Defence Intelligence', *in European Open Source Intelligence Workshop by European Union Information Sharing (EUFIS) in association with International Centre for Security Analysis*

Sites

1) Ackerman Robert (2006), 'Intelligence Center Mines open Sources', Armed Forces *Communications and Electronics Association,* http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=1102&zoneid=31 , 20 June 2008

2) BBC Monitoring: http://www.monitor.bbc.co.uk/index.shtml , 8 July 2008

3) Deep Web Technologies, 'The Deep Web', http://osint.deepwebtech.com/about-deepweb.html , 5 July 2008

4) Economist Intelligence Unit, 'Setting the Standard for Country Analysis and Forecasting', http://a330.g.akamai.net/7/330/25828/20051026163306/graphics.eiu.com/files/ad_pdfs/2005Methodology.pdf, http://www.eiu.com/site_info.asp?info_name=about_eiu&entry1=about_eiuNav&page=noads# , 14 July 2008

5) ESRI Press Release (2007), 'ESRI and Jane's Information Group Forge Strategic Alliance', *ESRI,* http://www.esri.com/news/releases/07_3qtr/janes-information-group.html , 31 July 2008

6) Jane's Information Group: http://catalog.janes.com/catalog/public/index.cfm, http://catalog.janes.com/catalog/public/html/defence.html , http://catalog.janes.com/catalog/public/html/security.html , http://catalog.janes.com/catalog/public/html/intelcentres.html , 30 July 2008

7) New York post, 'Terrorrockets.com-Google a weapon vs Israel', http://www.nypost.com/seven/10262007/news/worldnews/terrorrockerts_com.htm , 25 May 2008

8) Oxford Analytica, 'The Global Stress Points Matrix', http://www.oxan.com/GlobalStressPointsMatrix.aspx , 12 July 2008

9) Quiggin Tom (2006), 'Open Source Intelligence for National Security', *International Relations and Security Network (ISN),* http://www.isn.ethz.ch/news/sw/details.cfm?ID=16727, 7 June 2008

10) Relief Web, 'About ReliefWeb', http://www.reliefweb.int/rw/hlp.nsf/db900ByKey/AboutReliefWeb?OpenDocument , 9 June 2008

11) USA Today, 'Today's spies find secrets in plain sight', http://www.usatoday.com/tech/news/surveillance/2008-03-31-internet-spies_N.htm, 3 June 2008

12) US Army Foreign Military Studies Office Joint Reserve Intelligence Center, 'Intelink-U', http://fmso.leavenworth.army.mil/wbil/osisinfo.htm , 20 August 2008

13) Wait Patience (2006), 'Intelligence Units Mine the Benefits of Public Sources', *Government Computer News (GCN) Staff,* http://www.gcn.com/print/25_6/40152-1.html?page=1 , 15 June 2008

14) Wikipedia: http://en.wikipedia.org/wiki/BBC_Monitoring , 8 July 2008

Interview

1) Interview from Avital Johanan who is an analyst at Jane's Information Group, 29 July 2008

About the Author:

Harris Minas is an Intelligence Analyst in Sandstone S.A. in Luxembourg)

RIEAS Publications:

RIEAS welcomes short commentaries from young researchers/analysts for our web site **(about 700 words),** but we are also willing to consider publishing short papers (**about 5000 words**) in the English language as part of our publication policy. The topics that we are interested in are: transatlantic relations, intelligence studies, Mediterranean and Balkan issues, Middle East Affairs, European and NATO security, Greek foreign and defense policy as well as Russian Politics and Turkish domestic politics. Please visit: **www.rieas.gr (Publication Link)**