Belling the Cat

Investigative journalism versus traditional intelligence

Universiteit Leiden

Institute of Security and Global Affairs

Master thesis Crisis and Security Management
Student: Mick Berendregt (s2263351)
Institution: Leiden University
Thesis supervisor: G.G De Valk
Date: July 21, 2020
Wordcount: 19066

Table of contents

1.0 Introduction

On the 17th of July, 2014, around 12:15 PM, flight MH17 of Malaysia Airlines, started its journey from Amsterdam with Kuala Lumpur as its destination. After three hours, the Boeing 777-200, with 298 people on board, lost contact with the ground, flying approximately 50 kilometers from the Ukrainian-Russian border (De Volkskrant,2014). Within two hours it became clear that the plane had crashed on Ukrainian territory, with on sight footage showing that the crash had almost left nothing of the plane (Idem). At the time of the crash, the region in which the plane had crashed was involved in a serious conflict between the Ukrainian government and pro-Russian separatists Within a day, both parties blamed each other for taking down MH17. The Ukrainian president Poroshenko spoke of ''a terrorist act'', with the separatists on the other side denying any involvement claiming they would not be able to shoot down a plane at the given altitude. However, the spreading of the plane wreck across several kilometers of ground implied that the plane exploded at a high altitude (NOS, 2014). In the first weeks after the crash, the Dutch government gave priority to the salvaging of the bodies of the victims and securing evidence, the black boxes and the belongings of the victims. The Dutch Safety investigation board and the Dutch national forensic team landed on the 18th of July 2014 in Kiev, to investigate the crash site (NOS, 2014). This however, was hindered by the ongoing conflict between the Ukrainian government and the separatists, leading to the moving of bodies by separatists, the plundering of the crash site and destruction of critical evidence (NOS, 2014, Trouw, 2014, Trouw, 2014). Between the actual incident (July 17th) and the end of October 2014, multiple unsuccessful attempts had been made (De Volkskrant, 2014). Until the 31th of October 2014, Dutch and Ukrainian investigative teams were not able to get to the crash site and conduct a thorough research.

Besides securing evidence and the ongoing investigation in what exactly happened to flight MH17, the Dutch Safety investigation board requested for an investigation by the Supervisory Committee on the Intelligence and Security Services (CTIVD) on the possible knowledge of both Dutch military and general intelligence services (MIVD and AIVD) of the safety of the eastern Ukrainian region prior to the crash and to what extent these Intelligence services had shared this information with the involved airlines (De Volkskrant, 2015). A few weeks later, a Dutch investigative journalist radio program stated that prior and during the time of the crash, no representatives of the Dutch intelligence services were stationed in Ukraine due to capacity problems. This could have been the reason some airlines decided to not fly above the Ukrainian territory in conflict, while others like KLM and Malaysia airlines continued to do so. (Modderkolk,2015). Some would say, this was already the case in June 2014. The Dutch newspaper NRC (2014), reported that the Dutch general intelligence service (AIVD) faced an enormous capacity problem due to the growing threat of Islamic terrorism. Other core tasks had to be abandoned in order to combat the emerging threat of jihadists leaving to Syria to join ISIS. Three days before the crash, a Ukrainian delegation (including a Dutch diplomatic delegate) talked about the security in the eastern Ukrainian region. They spoke of an Antonov aircraft being shot down at 6,2 kilometers altitude. A report of the meeting was sent to multiple ministries including foreign affairs, defense and General affairs, but not to any airline nor the relevant ministry of Transport and Environment (Modderkolk ,2015). The CTIVD investigation followed at the request of the Dutch Safety investigation board, hence came to some important conclusions.

The Dutch Military intelligence services (MIVD) and the Dutch general intelligence services (AIVD), had the knowledge about the capabilities of the Russian armed forces to shoot down a civil aircraft and the fact they had no intentions to take down any civil aircraft. Both services had no information regarding the capabilities of the separatist forces to take down an aircraft on cruising altitude.

There were no indications of preparations aimed at civil aviation and no information of partner intelligence services was received of possible threats (CTIVD,2015).

Already in November 2014, an investigative journalist group named Bellingcat, published a report on the Buk missile launcher, that would have fired the missile that downed MH17. Using solely opensource intelligence (OSINT) and in particular intelligence/information gathered from social media (SOCMINT), Bellingcat was able to identify the made preparations for using the Buk missile launcher in a detailed manner (Bellingcat, 2014). The report showed that the Ukrainian separatists were in control of such a missile launcher: gathered evidence (mostly footage from social media) showed that the launcher was transported on the 17th of July towards the region where MH17 crashed. Three hours after the actual crash, it was moved again with one missile missing (Idem).

Bellingcat proved that the gathering, processing, analyzing and dissemination of intelligence, is no longer solely confined to the traditional public intelligence services such as the CIA or its British counterpart MI6. This raises questions on multiple levels. To what extent are investigative journalist groups, such as Bellingcat, able to carry out the same tasks as traditional public intelligence services? What are the strengths of investigative journalist groups in terms of the intelligence cycle, compared to traditional intelligence services and vice versa? Are there possible advantages and disadvantages of incorporating investigating journalist groups into the public domain, given the fact that Dutch intelligence services have to deal with a greater amount of threats?

1.1 Scientific and social relevance

As Best (2008) argues, the report of the 9/11 commission exposed the weaknesses of the traditional intelligence bodies because of being too complex and secretive. He states that although information regarding the threat posed by AL Qaeda to American soil was publicly available, intelligence services were not able to ‘’connect the dots’’. The report also recommended the formation of an Open Source intelligence agency, in order to bring the Intelligence Community (IC) into the information age. According to Degaut (2016), the IC faces an enormous challenge to cope with massive changes/developments in the uses and applications of information and communications technologies. These rapid changes and developments have strong effects on how intelligence collection, processing, analysis and dissemination should be handled. Increasing interconnectedness in every digital form accompanied with greater use of social communication, have reshaped every aspect of life.

Degaut (2016) argues that advances and improvements in ICTs not only created new opportunities but also new challenges and threats to intelligence services, by enabling not only governments, but also terrorist and criminal groups to conduct activities that could possibly harm national interests. The rapid change, increasing complexity and thus rising uncertainty of this threat environment forces the institutions that are responsible for providing information (the intelligence community) to diverse their tasks, in order to monitor every aspect. This means that in time, the tasks of the intelligence community have become more dynamic, diverse and thus more difficult (Fingar,2012).

Given these developments and the assumption that the Information Revolution will further interconnect the world as we know it today, the scientific relevance of this research lies in to what extent private investigative journalist groups such as Bellingcat are similar in their working compared to governmental intelligence organizations, in order to make statements about the potential of cooperation between these two.

Commissioned by the Ministry of Security and Justice, the USBO, the Department of Public Administration of Utrecht University, has conducted research on how the Dutch society and government have to deal with complex security challenges. The core concept within this research is the concept of ''the resilient and open society'' (Noordegraaf et. Al, 2019). This concept is a blend of the concepts: ''open society'' and ''resilient society''. In short, the former refers to a society where laws, customs and institutions are open to change. Members of the society can openly criticize its institutions and accompanied power structures, without the fear of prosecution (Noordegraaf et. Al,2019, p.31). The latter entails a society where people have the ability to cope with or to adapt to disturbances to the normal experienced condition (Idem). The Dutch National Security Strategy tells us that in protecting the national security, the Dutch government aims for a society-wide approach, where empowered and self-reliant citizens take their own responsibility, supported by a strong government:

> *''At the same time, this safety can no longer be achieved by the government alone. Business, civil society organizations and citizens also play an important role in ensuring national security and promoting resilience. The government has a coordinating role in this and must act in a recognizable, transparent and role-stable manner in the event of threats or risks''*
> (NCTV,2019, p.17)

Furthermore, the Dutch government is committed to early detection of risks signals and threats to the national security. This means information sharing between public parties and between public and private parties as much as possible promoted. However, this information sharing should be within the applicable legal frameworks and safeguards (NCTV,2019, p.17). Not only public services but also private parties can contribute to the resilience of society. In this way, intensified cooperation (sharing of information and monitoring of possible threats) between public and private intelligence services, can be regarded as a double-edged sword: it reliefs traditional public intelligence services of their many tasks and it enables the government to have their ''eyes and ears'' on every corner of the street. Thus, the societal relevance lies in gaining new insights into possible relationships of public and private parties in gathering intelligence, to protect the society for events such as terrorism at home, but also situations abroad, like the downing of MH17.

1.2 Research question

Against the background of the questions about the similarities between private and public parties in the collection, processing, analyzing and dissemination of information, the following research question has been formulated:

What are the similarities in the way of working between Bellingcat as a private investigative journalist group and governmental intelligence organizations, seen through the different stages of the intelligence cycle (organizational process), the collection of overt and covert information through the suspicious signs-model (sources of information) and collection methods (activities), illustrated by the case of MH17 and the report on the source of the separatists' Buk?

In order to answer the posed research question, the research question will be answered on the basis of three sub-questions that involve three concepts: one on the concept of the intelligence cycle (the organizational process of processing intelligence), two on the concept of different the different types of intelligence (collection methods, analysis) and three on the concept of the Suspicious signs model (the nature of the collected information, overt and covert information):

- ***The intelligence cycle:*** *''To what extent is Bellingcat similar to governmental intelligence organizations when looking at the organizational process of the intelligence gathering process?''*
- ***The different types of intelligence:*** *To what extent is Bellingcat able to use the same methods of collection and analysis compared to governmental intelligence organizations?*
- ***The Suspicious signs model:*** *To what extent is Bellingcat able to gather the same intelligence (overt and covert) in time and place compared to governmental intelligence organizations?*

2.0 Conceptual framework

In order to make a statement about to what extent Bellingcat is similar to governmental intelligence organizations, the decision has been made to divide the conceptual framework into three parts:

In the first section (2.1), in order to make claims about to what extent the production of intelligence in organizations such as Bellingcat are comparable to that of governmental intelligence organizations, the organizational process in the production of intelligence has been conceptualized through the concept of the intelligence cycle. The second section (2.2) discusses the intelligence concepts of collection methods (opposite to the scientific ones of document, interview and experiment), in order to look if organizations as Bellingcat are using similar collection methods compared to governmental intelligence organizations. The third section (2.3) examines to what extent Bellingcat is able to collect certain information at certain periods of time (the nature and time of the collected information) compared to governmental intelligence organization. For this we use the concept of Suspicious Signs as developed by Rademaker et. Al (2006).

In the conceptual framework, the three concepts will be further elaborated in order to be tested in the analysis.

2.1 The intelligence cycle: The organizational process of the production of intelligence

In order to make a comparison between Bellingcat and governmental intelligence organizations in the production of intelligence, the organizational process in the production of intelligence, is conceptualized through the intelligence cycle posed by Herman (1996). According to Herman (1996, p.285), the organizational process of the production of intelligence, as applied in the military setting, is a cyclical process and consists of 4 different phases: The *consumers* of intelligence indicate the kind of information needed, these indications are being translated by senior intelligence managers into *requirements*. The requirements serve as a guide for the *collectors*. The obtained information by the collectors (raw intelligence) is being analyzed and processed into finished intelligence by *analysts*. The finished intelligence is being distributed (disseminated) to the consumer, who can, in turn, define new requirements, state new needs and make adjustments in the intelligence program in order to improve effectiveness and efficiency (Idem). The described production process of intelligence can be translated into the diagram below.

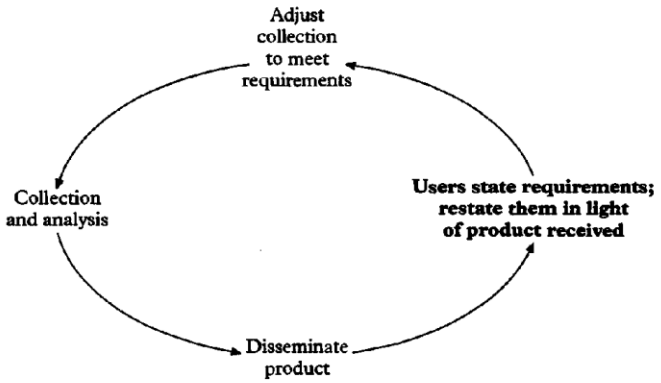


Figure 16 Military concept of the intelligence cycle

(*Source:* Herman, M. (1996). *Intelligence Power in Peace and War*. Cambridge University Press., p. 285)

2.1.1 Consumer (user) requirements and its limitations

According to Richelson (2015), the planning and direction of intelligence efforts are a product of the interaction between policymakers, who express their needs for information on a certain subject towards the senior intelligence managers. This entails the identification of the kinds of data needed and the assignment of the task of collection to the appropriate agency (Johnson,2007). Johnson (2007) states that behind this seemingly smooth and straightforward relationship, difficulties arise when informational needs are not being made clear/known to the producers of intelligence. According to Hulnick (2006), the notion that intelligence consumers provide guidance to the intelligence managers to begin the intelligence process, is an incorrect assumption and needs to be seen as an interaction to goes back and forth: *''Policy consumers do sometimes indicate their main concerns to intelligence managers, but often they assume that the intelligence system will alert them to problems, or provide judgments about the future''* (Hulnick,2006,pp.959-960). This means that informational needs of policymakers are sometimes never made known to the producers (Johnson,2007), hence the reason that senior intelligence managers have to learn what policymakers are up to and have to take initiative to obtain this information (Hulnick,2006). Thus, with essential and accurate data being swept along from the producer to the consumer, which results in complex series of interactions between different people and organizations and sometimes results in the loss of vital information (Idem).

2.1.2 Collection of information (raw intelligence)

Intelligence services use different type of methods to collect information (raw intelligence). According to Herman (1996), there are four classic types of data collection methods: Human Intelligence (HUMINT), Imagery Intelligence (IMINT), Signal Intelligence (SIGINT) and other smaller collection sources such as Satellite intelligence (SATINT), Radio Intelligence (RADINT) and Nuclear Intelligence (NUCINT). Given the fact that the subject of research operates within the digital domain of intelligence, focused on collecting information from Social Media networks, the choice has been made to add Social Media Intelligence (SOCMINT) to add to the list of collection methods. These different collection methods will be further discussed in a separate section.

2.1.3 Processing and analysis of information (from raw to suitable intelligence)

According to Biermann et. Al (2004), the processing and analysis of raw intelligence is an important part of the intelligence cycle, since an accurate situational awareness is essential prior to almost every decision and activity. The processing and analysis step of the intelligence cycle compromises five steps: *collation, evaluation, integration and interpretation* (Thibaut, Gareau and May, 2007). Collation involves the grouping, logging and structuration of information to provide a record of events, that enables intelligence officers to evaluate information in a more effective way. The evaluation step involves determining the credibility and reliability of information. From thereon, the information regarded as credible and reliable will be analyzed in terms of the identification of significant facts, comparing with already existent knowledge and other facts, in order to draw conclusions. The analyzed information will be integrated (the fourth step) into a larger perspective, by combining different sets of analyzed information to form a pattern of events or create a picture of the situation. The meaning of these patterns will be interpreted (step 5) and judged on significance, in line with the current body of knowledge.

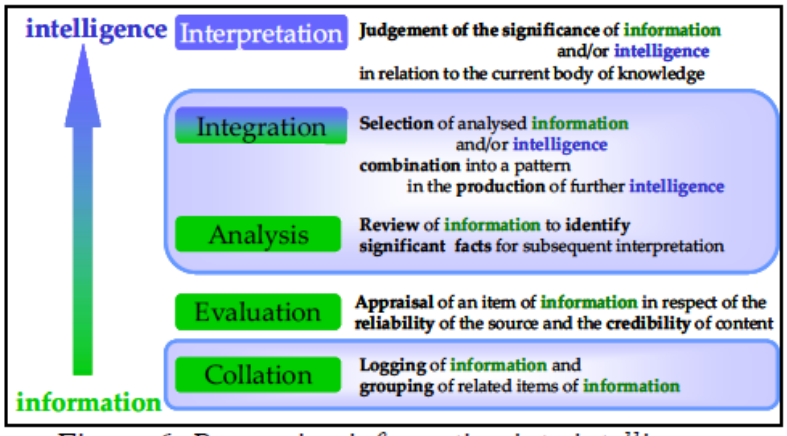


Figure 6: Processing information into intelligence.

Biermann, J. (2004). A Knowledge-Based Approach to Information Fusion for the Support of Military Intelligence. Research establishment for applied sciences Wachtberg-Werhoven (Germany) Ergonomics/Information Sys. P. 7-5

2.1.4 Dissemination of intelligence

The dissemination of intelligence makes up another (final) stage, but is very close related to the stated requirements by the consumer (first stage) and production of intelligence, since the intelligence cycle is a circular process (Herman,1996). Its aim is to deliver useful and user-friendly information towards the consumer. The disseminated information is mostly being used to reduce uncertainty and help the decision-makers to make more effective judgements about a certain subject (Marrin,2017). Therefore, as Herman (1996) argues, intelligence is being produced against time pressures and hence, dissemination is the intelligence Achilles' heel.

Marrin (2017) concludes that as a result of time pressure, the lack of knowledge about the capabilities of the intelligence services and the instrumental perception of decision makers towards intelligence services, intelligence is often used by decisionmakers to reassure their own believes and competing analysis will be ignored. Odom (2008, p.326) agrees: *'' Most operations staffs, commanders, and policy-makers have little or no idea of what intelligence one or another part of the Intelligence Community can provide. Thus they do not know whom to ask for what''.* Therefore, intelligence analysts have a responsibility to learn those things for their leaders and commanders, by being actively engaged in the formation of policies and the planning of military operations in order to make the process of requirements and dissemination more effective (Odom,2008).

In chapter 4.1, this thesis will analyze to what extent Bellingcat is similar to governmental intelligence organizations when looking at the organizational process of the intelligence gathering process. In other words: the intelligence cycle and its distinct phases of processing the gathered intelligence, will be tested on Bellingcat and the case of MH17, in order to look to for similarities.

2.2 Collection Methods and analysis

In order to be able to analyze to what extent investigative journalist groups as Bellingcat, use the same collection methods for intelligence as other intelligence organizations, the different collection methods must first be examined in terms of the actual collection methods and its characteristics, source validation and the relationship towards investigative journalist groups. According to Sienkiewicz (2015), most of the researchers of Bellingcat are voluntarily contributing in research in the form of crowdsourcing. According to Stottlemyre (2015), crowdsourcing intelligence can be described as: '' *Collecting information that was originally gathered by humans.* (Stottlemyre,2015, p.583). Stottlemyre (2015), in accordance with Herman (1996), argues that there are five traditional intelligence collection disciplines: human intelligence (HUMINT), open source intelligence (OSINT), signals intelligence (SIGINT), measurements and signatures intelligence (MASINT), and geospatial intelligence (GEOINT).

HUMINT and OSINT, as Stottlemyre (idem) argues, are achieved primarily through analysis gathered by humans, and therefore can be applied to the crowdsourcing environment, what in turn, relies entirely on human activity. Furthermore, Stottlemyre (2015) states that although some types of information appears to be GEOINT (for example locational metadata associated with other online activities, or Imagery downloadable from open sources), all crowdsourced information is presumed to be collected, produced and disseminated by individuals through open sources and therefore a part of the realm of OSINT.

On the basis of this division, the choice has been made to select HUMINT and OSINT as the primary methods of interest. Imagery intelligence (as a part of GEOINT) and Social media Intelligence (SOCMINT) will be handled as a part of OSINT. Although this is not the common distinction made between the different types of intelligence, this distinction can be justified based on the nature of an organization like Bellingcat, given that it can be seen as a crowd-sourcing platform.

2.2.1 Human Intelligence (HUMINT)

According to Herman (1996), HUMINT is intelligence obtained by people and can be regarded as the oldest form of data collection. Of all intelligence collection methods, HUMINT can be regarded as the best source to know the ''intent'' of another (Dillon,1999). A great part of human intelligence is collected from information that is available in the open domain in order to gather information about

threats that face the homeland and to help leaders with data that can help to advance national interest (Johnson,2010). Through the practice of espionage or clandestine human intelligence, actors try to ''steal'' secrets from another in order to get a better understanding about possible threats and opportunities.

The pyramid of Herman (1996) provides us a useable insight from a wide range of possible sources, ordered from non-sensitive sources at the base to high-sensitive sources at the top (see figure below):

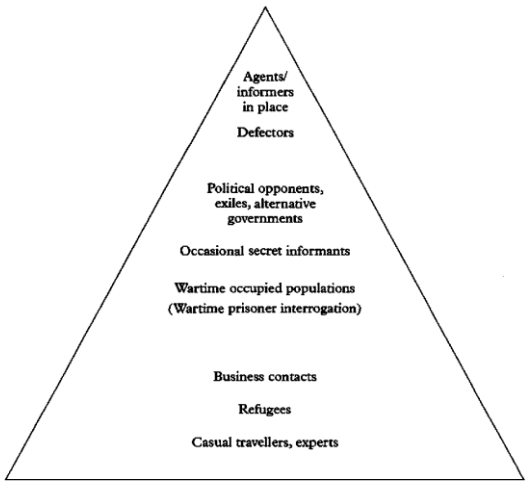


Figure 7 Humint's pyramid of source sensitivity, quantity and value

(Source: Herman, M. (1996). *Intelligence Power in Peace and War*. Cambridge University Press., p.63*).*

Validation of HUMINT-sources and intelligence

According to Herman (1996), HUMINT has a reputation of unreliable information. HUMINT-sources and therefore information is and has always been subject to human frailties: the ''managing'' authority of these agents can never count on the reliability of their sources. The controller can never be completely sure that reports of their agents are distorted, or provided with deceptive material when they are working as double agents. According to Irwin and Mandel (2019), NATO-members are using the admiralty coding scheme in order to determine whether the obtained information is reliable. This coding scheme is divided into two different schemes': The reliability of the HUMINT-source and the reliability of the obtained information from that source:

Table 7-1: NATO AJP 2.1 2016 Source Reliability and Information Credibility Scales [9].

Reliability of the collection capability		Credibility of the information	
A	Completely reliable	**1**	Completely credible
B	Usually reliable	**2**	Probably true
C	Fairly reliable	**3**	Possibly true
D	Not usually reliable	**4**	Doubtful
E	Unreliable	**5**	Improbable
F	Reliability cannot be judged	**6**	Truth cannot be judged

Table 7-2: NATO STANAG 2511 Source Reliability Scale [10].

Reliability of source		
A	Completely Reliable	Refers to a tried and trusted source which can be depended upon with confidence.
B	Usually Reliable	Refers to a source which has been successful in the past but for which there is still some element of doubt in a particular case.
C	Fairly Reliable	Refers to a source which has occasionally been used in the past and upon which some degree of confidence can be based.
D	Not Usually Reliable	Refers to a source which has been used in the past but has proved more often than not unreliable.
E	Unreliable	Refers to a source which has been used in the past and has proved unworthy of any confidence.
F	Reliability cannot be judged	Refers to a source which has not been used in the past.

Source: Irwin, D., & Mandel, D. R. (2019). Improving information evaluation for intelligence production. *Intelligence and National Security*, *34*(4), 503-525.

The quality of the obtained information via HUMINT-sources are highly dependent on many variables. Irwin and Mandel (2019) state that the reliability and credibility of information evolves around the following factors: *Credibility,* internal and external consistency, risk of denial and deception, timeliness and recency and unusual absence of evidence. *Validity:* circumstances under which the evidence has been gathered, quality of source's bona fides and sensor capabilities. Validation of information often involves triangulation with the use of other competitive sources in order to determine credibility (Idem). This results in the following information credibility scheme:

Credibility of information		
1	Confirmed by other sources	If it can be stated with certainty that the reported information originates from another source than the already existing information on the same subject, it is classified as "confirmed by other sources" and is rated "1".
2	Probably true	If the independence of the source of any item or information cannot be guaranteed, but if, from the quantity and quality of previous reports its likelihood is nevertheless regarded as sufficiently established, then the information should be classified as "probably true" and given a rating of "2".
3	Possibly true	If, despite there being insufficient confirmation to establish any higher degree of likelihood, a freshly reported item of information does not conflict with the previously reported behaviour pattern of the target, the item may be classified as "possibly true" and given a rating of "3".
4	Doubtful	An item of information which tends to conflict with the previously reported or established behaviour pattern of an intelligence target should be classified as "doubtful" and given a rating of "4".
5	Improbable	An item of information which positively contradicts previously reported information or conflicts with the established behaviour pattern of an intelligence target in a marked degree should be classified as "improbable" and given a rating of "5".
6	Truth cannot be judged	Any freshly reported item of information which provides no basis for comparison with any known behaviour pattern of a target must be classified as "truth cannot be judged" and given a rating of "6". Such a rating should be given only when the accurate use of higher rating is impossible.

Source: Irwin, D., & Mandel, D. R. (2019). Improving information evaluation for intelligence production. *Intelligence and National Security*, *34*(4), 503-525.

4.2.2 Open Source Intelligence (OSINT)

Within the intelligence community, Open Source intelligence (OSINT) is information collected from public available sources that has been deliberately discovered, discriminated and disseminated to a select audience to answer a certain intelligence question (Steele,2007). These publicly available information can be used by a great variety of individuals for many different goals (Steele,2007). According to the NATO Open Source Intelligence Handbook (2001), these public available sources are mainly the traditional media sources as we know them today: radio, television, newspapers, journals, internet (including social media), commercial databases and video. Burke (2007) states that this kind of open data can be extremely useful and is often the only mean of penetrating covert networks. According to Hribar et. Al (2014) intelligence services and its personnel are capable of advanced use of OSINT: they are familiar with specialized sources of publicly available data, advanced techniques to acquire this data and have the analytical skills for successful processing, exploitation and analysis of great amounts of data.

Imagery Intelligence (IMINT)

As well as HUMINT, Imagery Intelligence is part of the intelligence collection methods (Herman,1996). According to Kovarik (2011), IMINT is a contested concept and therefore, no definite definition has been reached in the field of intelligence. According to the United States Marine Corps (hereafter USMC) (2002) imagery is: ''*the representation of objects reproduced electronically or by optical means on film, electronic display devices or other media'' (USMC, 2002, p.1)*. Therefore, we can assume that IMINT is information/intelligence derived through the collection and analysis with use of the former. Principle sources for IMINT are satellites, manned aircrafts, radar systems, unmanned aerial vehicles numerous sorts of cameras and commercial imagery (Idem).

This intelligence about the enemy and/or operational environment, is used in order to reduce uncertainty, identify opportunities for possible success, to make an outline about the enemy's intent and to reach decisive success (USMC,2002, p.3). In order to fuse the imagery into useful information, specifically trained personnel, adequate time and sophisticated equipment are required (Kovarik,2011). Herman (1996) makes an important distinction between imagery intelligence based on intelligence collection and non-intelligence collection. Photography and foreign television broadcast, which are open sources, can possibly provide material for specialist imagery examination, in the same way as newspapers and other open sources can be of any value to HUMINT operations. Herman (1996) states that given the improvements of commercial satellites and the improvement in the resolution of other commercial open source imagery, states do seek more control over these sources.

Validation of IMINT-sources and information

According to Diamond (2001), imagery can detect and or identify and locate specific unit types, equipment, from which analysts are able to analyze enemy capabilities and movements. It can also be used for updating maps and to enhance the knowledge of a specific region only known by traditional maps. When traditional maps are not available, IMINT is used as a substitute: the most common application of by constructing imagery mosaics: a combination of two or more overlapping photographs that can be combined to get a single picture (Idem). Imagery, accompanied with MTI (moving target indicator) can provide (satellite) pictures of an entity's movement by indicating its speed, location and direction of travel. Most imagery analysts use combat assessment imagery to confirm destruction, determine the percentage of destruction or whether the target was unaffected

(Idem). According to Kovarik (2011, p.51), the image analyst routinely conducts several tasks which usually involve detection, localization, recognition, identification, listing, comparison, interpretation, understanding and prediction. Besides these common tasks, Kovarik (2011, p.52) names feature extraction as an important technique of manual IMINT analysis. Feature extraction entails the following techniques: Classification (the assignment of objects, features or areas to classes based on their appearance on the gathered imagery), enumeration (listing or counting discrete items which are visible on the imagery), measurement (ranges from a simple visual estimate of the size, shape and color of an object to detailed measurement and calculation of distance, height, volumes and areas and also scene brightness or density), and delineation (delineate, or outline, regions as they are observed on images. It involves the art to separate distinct areal units that are characterized by specific tones and textures, and to identify edges or boundaries between separate areas). Herman (1996, p.76) agrees, as he has formulated a similar approach of IMINT analysis: ''*Photo-interpretation is still largely a human skill based around 'five S's': size, shape, shadow, shade and surrounding objects''*. According to Montgomery et. Al (1980), the intelligence products which derive from IMINT may support a diversity of missions, including basic intelligence, indication and warning, targeting or direct support. The scope and form of these missions vary between strategic and tactical missions. The shared denunciator between these two types of missions is the timeliness. Montgomery et. Al (1980), have defined this timeliness into three distinct phases:

First phase: the first phase contains rapid imagery analysis and reporting of newly acquired information within specified time. This phase identifies changes or activity of immediate significance. According to Global Security (2020) first phase analysis results in an initial phase imagery report (IPIR).

Second phase: This phase contains the imagery analysis which is a detailed exploitation of newly acquired imagery. This phase can be regarded as a supplemental imagery report (SUPR) (Montgomery et. Al, 1980).

Third phase: Third phase imagery analysis is the detailed analysis of all available imagery. This phase provides an organized detailed analysis of an imagery target or topic, using IMINT as the primary data source, but combining this data with other sources as appropriate (Montgomery et. Al,1980).

In short, the phase in which the report is written has implications for the way in which IMINT analysis can take place. According to this theory, this means that at every later stage the predictive factor gives way to the explanatory factor. In order for a report to be predictive, rapid analysis of intelligence is needed. Since intelligence services are built around the assumption of knowing the capabilities and motives of another in order to make predictions and to prevent possible threats, it can be stated that phase 1 and partly phase 2 (depends to the extent one is able to collect and analyze imagery in a fast and detailed way) can be regarded to the predictive (and therefore primary) domain of IMINT-analysis, practiced by intelligence services. Phase 3 involves more or less explanatory (investigative) research and is therefore research of secondary nature within the domain of intelligence services. Thus, in order to make a statement about to what extent a report can be regarded as a report that resides in the domain of intelligence services, one has to determine the phase in terms by looking at the timeliness and the detail of the analysis in the report.

Social media Intelligence (SOCMINT)

According to Omand, Bartlett and Miller (2012), we live in the age of a rapid transfer from people's lives (interactions, relations, identities, arguments, etc.) onto a new type of public/private sphere: the world of social media. They state that this transfer is happening on an unprecedented scale. Bartlett and Miller (2013) argue that already in 2013, 1.2 billion people were increasingly sharing information about ourselves and our friends, to participate into different groups/communities and to ''share'' our likes and dislikes, movements, thoughts and transactions. Through mediums such as Facebook, LinkedIn, Instagram and VK-network, an innumerable amount of data is being shared across the globe. The greater interconnectedness of people around the world, not only creates new threats to the traditional intelligence community, but also offers a great new source of intelligence, since people tend to share more of their identity online in time (Lombardi, Rosenblum & Borato, 2015, Degaut, 2016). Given the great amount of data produced and being shared, different options arise for decision-makers in the use of the collected data in order to reduce ignorance. These options include ways to improve the information flow between the government and citizens in the form of crowd-sourced information and for research and understanding of societal problems.

Next to the more analytical usage of social media intelligence, information can also be used to generate operational intelligence for law enforcement, that could help identify criminal activity, indicate early warnings of outbreaks of disorder and provide information and intelligence about groups and individuals that may pose a threat to national security (Omand, Bartlett and Miller, 2012, Bartlett and Miller, 2013). The use of SOCMINT gives governments the ability to collect and cluster social media in a way that could possibly indicate and describe unfolding events. According to Power, Robinson and Cameron (2014) it provides essential insights into groups, their behavior, beliefs and activities. Using techniques such as language processing, event detection, data mining accompanied with predictive analysis (analyzing large datasets to find dynamics, interactions and causal connections) and manual analysis, SOCMINT is a highly differentiated method of analysis and therefore suitable for incorporation into different levels of the decision-making process (Bartlett and Miller, 2013). Dover (2020), states that within the field of SOCMINT, the contestation between government, the ill-informed and speculative, and the adversary communicator attempting to do the digital variant of denial and deception, are likely to get worse, and therefore the role of intelligence agencies is , focused on bulk interception and analytical techniques, to identify those actors. The greater focus of intelligence services on the analysis of large (bulk) datasets rather than on manual analysis has negative implications for the capabilities of the intelligence services to detect early forms of online radicalization and civil unrest: posts on Twitter and Facebook are mostly unstructured and informal and often slip through the automatic detection filters (Agarwal & Sureka, 2015). This means that intelligence services can detect patterns of behavior within large groups, but have problems when it comes to subtle and unstructured SOCMINT. In order to determine whether Bellingcat is similar to intelligence services in the collection and analysis of SOCMINT, the different SOCMINT collection and analysis techniques will be discussed.

Bartlett and Miller (2013) regard the following collection techniques as the most significant, capable of reducing ignorance and improving decision-making for the purposes of counter-terrorism and as a function of the traditional intelligence services: natural language processing, event detection, data mining and predictive analytics, social network analysis, manual analysis (or netnography) and solicited crowdsourced analysis. These techniques and conceptualizations of Bartlett and Miller (2013) will be briefly outlined below:

SOCMINT collection and analysis techniques

Natural language processing

A branch of artificial intelligence involving the computational analysis (often using machine learning methods) of 'natural' language as it is found on social media (Bartlett and Miller,2013).

This commonly involves the ability of multiple computational language programs, artificial intelligence and computational linguistics to find patterns in language.

Event detection

The statistical detection analysis of social media streams to identify offline 'events', whether natural, political, cultural, commercial or emergency to provide situational awareness, especially in dynamic and rapidly developing contexts (Bartlett and Miller,2013). This technology tries to identify events by observing phrase usage over time that indicate that an event may be occurring.

Data mining and predictive analytics

The statistical analysis or 'mining' of unprecedentedly large ('big data') datasets, including social media and other 'big' or open data sets (such as Census data, crime, health, environmental and transport data), to find the dynamics, interactions, feedback loops and causal connections between them (Bartlett and Miller,2013). In short, this means that previously as harmless and not valuable considered data, as mentioned above, can be combined to find certain valuable patterns in people's behavior. Think of online buying behavior, search terms on google, visited websites and election results, that may indicate and point towards a certain situation that is unfolding.

Social network analysis

The application of a suite of mathematical techniques to find the structure and topography of the social networks found on social media. These networks are then subjected to analysis, which can identify a range of implications and conclusions (including predictive ones) on the basis of the characteristics of the network structure and type (Bartlett and Miller,2013). This mostly involves 'data-mapping', where data is combined into a map to provide an oversight within a dynamic and rapidly developing situations (Oard and Webber,2012).

Manual analysis / 'netnography'

Drawn from qualitative sociology and ethnography, this is a broad collection of manual approaches to collecting and analyzing data concerning social media data. It often aims for depth over breadth in order to reveal and untangle the hidden, obscured, overlooked or contingent social significances, meanings and subjectivities experienced by individuals on social media (Bartlett and Miller,2013). In short, this can be related to traditional HUMINT-analysis in the new digital world.

Solicited / 'crowd sourced' insight

Refers to the emerging practice of a number of public and private agencies to use social media to ask citizens or social media users for information directly (Bartlett and Miller,2013).

Validation of SOCMINT-sources and information

During the validation of this gathered intelligence, the authors argue that this information should be reviewed with great caution: since SOCMINT is the digital version of HUMINT, it is prone to contain misleading information, which may involve the recirculation of half-truths, mistakes and distortions (Omand, Bartlett and Miller, 2013). According to Bartlett and Miller (2013), there are lots of examples of inaccurate information or misinformation being used by specialists. Wrong tweets by trolls or bots are have been picked up, believed and reported on the biggest news outlets. They state that in many respects, the validation of information (intelligence) that has been retrieved for Social Media would require the same standards as for HUMINT-sources and information: track record, known capabilities, motivations etc. Different techniques can be used, such as cross-referencing against landmarks and checking unique URL's. Different geo-locations, IMINT (photographs, videos, other imagery), tweets and status updates can be combined into a map (Oman, Bartlett & Miller 2012).

In chapter 4.2, this thesis will analyze to what extent Bellingcat is able to use the same methods of collection and analysis compared to governmental intelligence organizations. In other words: this thesis will analyze the extent (the width and depth) to which Bellingcat is able to cover each form of intelligence gathering and analysis, compared to governmental intelligence organizations.

2.3 Suspicious signs model

In order to be able to address to what extent investigative journalist groups such as Bellingcat are able to collect overt and covert information compared to governmental intelligence organizations, the Suspicious Signs-model (hereafter: SSM) of Rademaker et. Al (2006) will be used. Commissioned by the Dutch Ministry of the Interior and Kingdom Relations, Rademaker et. Al (2006) created a new thinking- and data model in order to proactively create a good information position on potential threats and risks. The SSM consists of four distinctive phases leading up to violent action: *Occasion, Trigger, Rumbling, Work-up process* and the actual violent action. Each phase has different suspicious signs. Subsequently, different collection methods (in informational sense) need to be applied. With each successive phase, the collection methods are becoming increasingly operational and takes more capacity of the involved intelligence organization. Therefore, the authors recommend prioritization on the base of severity and probability.

These distinct phases and the working of the model will be further discussed below.

2.3.1 Suspicious signs phases

Occasion

The first phase can be regarded as a breeding ground for the four (including violent action) subsequent phases of the SSM. According to Rademaker et. Al (2006), the first phase requires a multidisciplinary approach to gain insights into trends that may have repercussions for threats to people and objects on a long-term base. Therefore, the authors argue that trend-analysis is needed. Examples of *occasions* are: *disasters, economical decisions, historical events, public claims* and *announcements*.

Trigger

The first phase, may result in a conviction of an individual or group, that something has to happen or not. Within phase two, a trigger can be regarded as a suspicious sign. The entry of an actor or factor that rises unrest can be regarded as the trigger. Examples of triggers are: inspirators (individuals or groups that take a stance and plea for action), governmental (political) decisions that lead to commotion, violent actions and / or public statements during the Work-up process that lead to persons or groups also wanting to manifest themselves (will be further elaborated in the 4th phase). Trends with relevance to the Trigger phase are a hardening relationship between the citizen and the state and a rise in politically motivated activism (Rademaker et. Al, 2006). According to the authors, the following analysis techniques should be taken into account:

''Behavioral science analyzes and profiling of groups but also individuals and thereby mapping which types of groups or individuals trigger on the occasions. But also matching these results with known risk groups and individuals.'' (Rademaker et. Al, 2006, p.33)

Rumbling

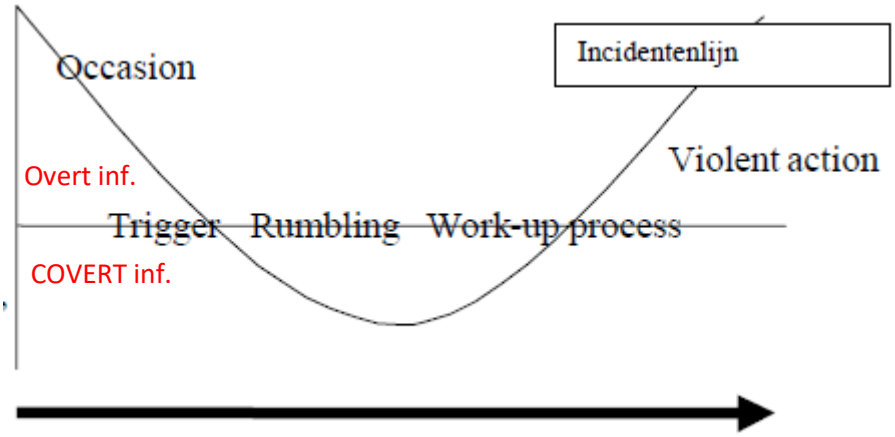
During this phase, the triggers from the third phase are being translated into first premature forms of action. Dissatisfaction of individuals or groups, with the current situation, leads to forms of demonstrations, protests, statements in the media and political actions. According to the authors, the following types of analysis are required: ''*Trend analysis of all kinds of media expressions. Skill and scanning capacity for the efficient tracking and analysis of open sources, but also quantitative analysis of data traffic and data mining to identify patterns.. In addition, human intelligence and signal intelligence and other forms of intelligence must certainly contribute to this.'' (Rademaker et. Al, 2006, p.35)*

Working-up process

Before a certain individual or group comes to the actual violent action, preparations must be made. In this phase, the emphasis lies on signs that contribute to the working-up process towards violent action. Examples are: *The concentration of resources (material, financial and logistics), recruiting, reconnaissance, training, planning of violent actions.* The authors state that the following analysis techniques are needed to follow the working-up process: '' *Tracking suspicious persons, travel patterns, contacts and meetings, the use of suspicious infrastructure, etc… In this phase, analysis in methods and techniques of potential perpetrators and groups will be carried out. In addition, human intelligence and other forms of intelligence will have to be used in addition to the methods from the previous phases.'' (Rademaker et. Al, 2006, p. 37)*

2.3.2 Process

Although each phase has distinct characteristics, each phase is a product of or at the base of the other. This means that each phase influences the former and simultaneously the subsequent phase. Therefore, no absolute divide can be made between the phases. The five phases combined with to what extent these suspicious signs are ''visible'' for intelligence collection methods, leads to the following scheme:



Source: Rademaker et. Al (2006) *Denk- en datamodel Suspicious Signs*. Clingendael: Den Haag, p.38

This scheme tells us that between phase 2 and phase 4, open-source intelligence is not possible, or at least very difficult to obtain. The authors state that more covert collection methods are needed between phase 2 and 4 like IMINT, SIGINT and traditional HUMINT. Furthermore, the authors state that:

> *''It has been found that with regard to the suspicious signs phases Trigger, Rumbling and partly also Work-up process, it is often difficult to collect information from historical files based on open sources, since these cases usually do not give rise to media reports. This means that a significant portion of the data collection and processing capacity will be required to identify many seemingly insignificant or unsuspected data'' (Rademaker et. Al, 2006, p.41)*

Given the assumptions that have been made, this would have implications for investigative journalist groups such as Bellingcat. These organizations rely almost entirely on intelligence gathered from open sources (OSINT). In this sense, it would on the one hand mean that these types of covert intelligence are still solely confined to the governmental intelligence organizations, who have the capacity, (covert) collection methods and resources to find the triggers, rumbling up and work-up process to the actual violent action. On the other hand it would mean, that if Bellingcat is able to cover these phases, they would cover each phase, just like the governmental intelligence organizations and subsequently, what used to be ''covert'' phases leading up to the actual violent action can be explored with the use of Open Source intelligence.

In chapter 4.3, this thesis will analyze to what extent private investigative journalist groups are actually able to collect and analyze this overt and covert information. In other words: The Suspicious signs model will be tested, based on Bellingcat's MH17 report.

3.0 Methods

There are many different ways to conduct a literature research combined with a single case-study. According to Bryman (2012), the basic case study entails an intensive and detailed analysis of a single case. Looking at the research subject in the form of Bellingcat and what we want to know (the extent to which intelligence is being collected, processed an analyzed), the choice has been made to incorporate the method of process tracing within this single case study. This choice will be further elaborated below.

3.1 Process tracing

Process tracing will be used in order to be able to make statements about to what extent Bellingcat, follows the intelligence cycle, use the same collection methods and is able to generate the same information (overt and covert). This method, as Mahoney (2012) argues, can be used as a method that analyzes hypotheses about the causes of a specific outcome within a case. This means that underlying factors can be explained with the use of process tracing. Process tracing is a technique where one looks for evidence within a case in order to accept or reject the given hypotheses. Brady & Collier (2010) argue that this can be compared to solving a murder case, by involving meticulous investigation into small pieces of evidence that may explain the actor's motives, opportunities and goals:

> *''There is no guarantee that researchers will include in their analyzes the variable (s) that actually caused Y, but process tracing backward from observed outcomes to potential causes — as well as forward from hypothesized causes to subsequent outcomes — allows researchers to uncover variables they have not previously considered. ''* (Brady & Collier, 2010, p. 3).

According to Collier (2011), the advantages of process tracing are that it is able to identify and describe new political and social phenomena, evaluate given explanatory hypotheses, discover new hypotheses and provide insight into the causal mechanism. Thus, process tracing enables one to look back for explanatory factors that could have had an influence on the given outcome within a single case.

3.2 Data

Mainly secondary scientific literature such as books, articles, reports and journals will be used as the basis for the thesis. The reports from various research institutions will mainly be used as a link between theory and reality. Media and/or news reports will be treated with great caution, as these reports may be biased and therefore affect the outcome of the investigation. However, media and news reports can supplement to the provision of background information.

3.3 References

Special attention must be paid to the way of referencing that will be handled within this thesis. The APA reference style will be used for the majority of the thesis. However, the Bellingcat report also references at sources by using URLs. Due to the ease of verifiability and therefore greater transparency of the thesis, the choice has been made to leave the URLs in the text.

4.0 Analysis

In order to get a better view of investigative journalist groups such as Bellingcat and their relationship towards traditional public (governmental) intelligence services, their activities and subsequent strongpoints, the analysis has been structured as followed: First, in chapter 4.1, the extent to which Bellingcat is similar to governmental intelligence organizations in the organizational process of the intelligence gathering process and analysis will be tested using the intelligence cycle and apply/compare these distinct features as described in the conceptual framework on/with the organizational process of Bellingcat. Second, in chapter 4.2, the described characteristics of the different forms of the intelligence collection methods and analysis will be held next to the report on the origin of the separatists' Buk made by Bellingcat, in order to test the breadth and depth in the use of these collection forms and forms of analysis, compared to that of governmental intelligence organizations. Third, in chapter 4.3, the Suspicious signs model, as described in the conceptual framework, will be held next to the report in order to look whether the assumptions made in the model hold up and to test the extent to which Bellingcat is able to cover the phases of the model compared to governmental intelligence organizations.

4.1 Sub question 1: *To what extent is Bellingcat similar to governmental intelligence organizations when looking at the organizational process of the intelligence gathering process?*

4.1.2 Introduction

According to Toler (2018), three large investigative journalist groups emerged during the Ukrainian conflict, including Bellingcat. Bellingcat has been founded by Eliot Higgins, after years of successful blogging, on 14th of July 2014 after a crowdfunding campaign (Bellingcat,2019). The emergence of these investigative journalist groups must be seen in the light of the earlier described information age and the democratization of the internet, the Ukrainian conflict and the subsequent (dis)information war between the Russian oriented eastern and the western media (Ilyuk,2019). The aim of digital investigative journalism is to bring transparency, find lost structures and processes in a world of ostentatiously displayed data (Lehren,2018; Ilyuk,2019). Immediately after its founding, the group started investigating the downing of MH17 as an attempt to reconstruct the chain of events related to the Boeing crash, which is the most well-known investigation of the group so far (Ilyuk,2019). According to Toler (2018), Bellingcat distinguishes itself from other investigative journalist groups with its topics of interest, organizational structure and research methodology. Contrary to the other two investigative journalist groups (Inform Napalm and Conflict Intelligence Team), who are solely focused on conflict-related investigations, Bellingcat uses Open Source intelligence (OSINT) to investigate a multitude of topics, such as: corruption, environmental issues and information security (Bellingcat,2019). Furthermore, Bellingcat differs substantially from other investigative groups looking at research methodology which in turn, has important implications for the organizational structure of the investigation group: their extensive use of crowdsourcing in the collection of data and analysis of information (Toler,2018). With the use of crowdsourcing and therefore the ''burden-sharing'' of the collection and verification of data among contributors, who are spread out across the world, Bellingcat enables itself to use a plurality of world views and political ideologies, which in turn can be beneficial to the objectivity of the research (Ilyuk,2019 ; Toler,2018).

This part addresses to what extent Bellingcat and its organizational processing of gathered intelligence is similar to that of the traditional intelligence services. In this part of the analysis, the intelligence cycle will be compared to the organizational process used by Bellingcat. It will be examined to what extent these two processes can be compared and what the advantages / disadvantages are, relative to each other. First, the organizational process of Bellingcat will be discussed. Second, the organizational process of Bellingcat (EDRM-model) and the traditional intelligence cycle, as discussed in the conceptual framework, will be compared.

4.1.3 Bellingcat and the EDRM-model

According to Bellingcat, in order to preserve the high quality of the investigation and the consistency of the process, the methodology of the verification of open source intelligence is being handled with the use of the EDRM- (electronic discovery reference) model (Bellingcat,2019). Electronic discovery can be described as the process in which any electronic data is sought, located, searched and preserved with the intent of using it as evidence in civil or criminal legal proceedings (Billard,2009). The EDRM-model consists of 6 e-discovery phases: information management, identification, preservation and collection, processing review and analysis, production and presentation (Billard,2009, Oard & Webber,2012). These phases are chronologically depicted in the figure below, but the process itself does not have to follow all 6 phases, some phases maybe iterated, before going onwards to the next phase. Each phase will be discussed below.

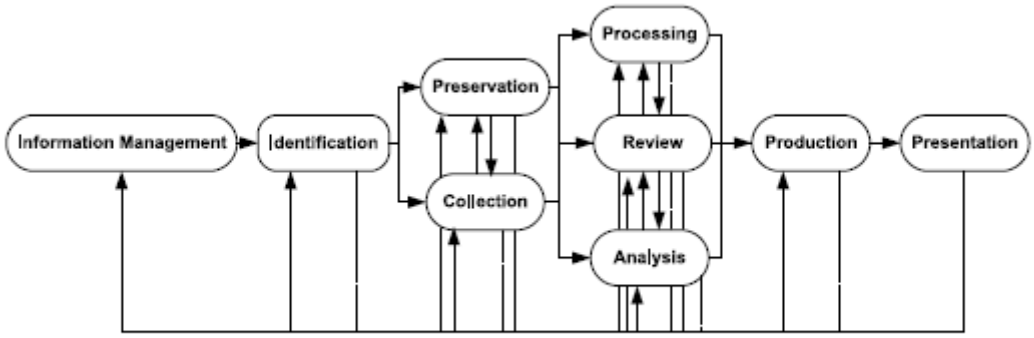


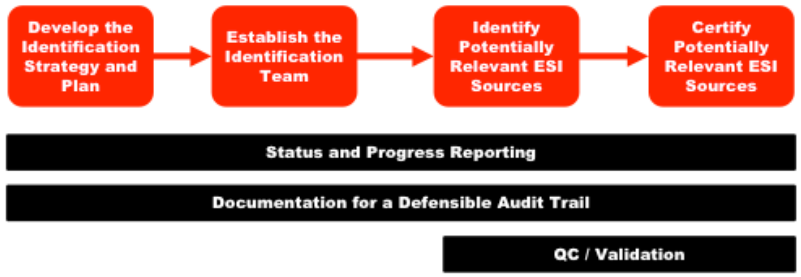
Figure 1. Electronic Discovery Reference Model.

Source: Billard, D. (2009, January). An extended model for e-discovery operations. In IFIP International Conference on Digital Forensics (pp. 277-287). Springer, Berlin, Heidelberg.

According to Billard (2009), Oard and Webber (2012), the first phase ''information management'' is not necessarily a part of the e-discovery itself, but in encompasses all pre-process activities prior to the e-discovery itself. This means that the left-most phase of the model can also include activities that are outside of the control of the actual e-discovery team such as policy, legal and regulatory goals (Oard and Webber (2012). The second phase of ''identification'' involves the location of possible evidence sources (Billard,2009). According to the EDRM-model website, the identification process is two-sided: On the one side, the identifying process encompasses the identification of key players, custodians, location of data and the traceability of data. On the other side, it also means identifying key people involved in the e-discovery process (www.edrm.net). The identification phase takes place around four main phases: Developing the Identification Strategy and Plan, Establish the Identification Team, Identify Potentially Relevant ESI Sources and Certify Potentially Relevant ESI Sources (Idem).

According to Oard and Webber (2012), the identification phase can be divided into two different types of activities: first, information systems that may contain vulnerable information need to be identified. This activity is called ''Data mapping''. It produces a ''data-map'' that depicts the information stores and information flows.

Second, decisions need to be made, and agreed between the parties, about which systems information will be collected from, and what restrictions will be placed on the collection process (Oard and Webber, 2012). The identification process is shown schematically below:



Although represented as a linear workflow, moving from left to right, this process is often iterative. The feedback loops have been omitted from the diagram for graphic simplicity.

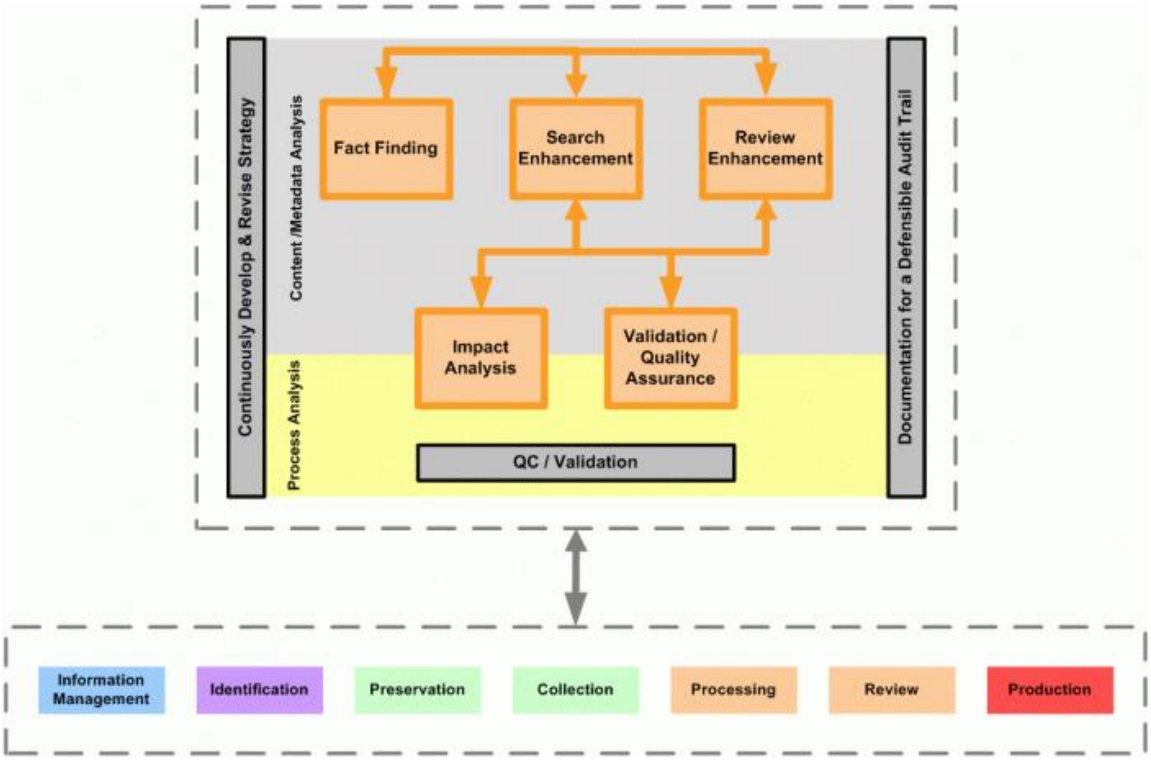
Source: https://www.edrm.net/resources/frameworks-and-standards/edrm-model/identification/

The third phase, preservation and collection, entails the preservation and collection of potential evidence. During this phase, exact copies of the evidence that is deemed to be relevant, are being made (Billard,2009). The ''collection'' part is quite simple: getting what is decided to get. According to Webber and Oard (2012), this usually involves ordinary means (issuing queries to operating databases), specialized means for restricted data and forensic techniques to recover inaccessible information. Preservation involves three basic functions: maintaining the bit stream, maintaining information that is necessary to interpret the former and maintaining evidence of authenticity. In other words: Bellingcat uses a wide array of ordinary, specialized and forensic tools to gather the evidence from Open Source channels, that it deemed to be relevant. These techniques vary from tweet saving applications to geolocation apps, geospatial data, Satellite imagery websites and commercial registries. These techniques are outlined below:

Source: Bellingcat online investigation toolkit (https://docs.google.com/document/d/1BfLPJpRtyq4RFtHJoNpvWQjmGnyVkfE2HYoICKOGguA/edit)

The fourth phase of ''processing, review and analysis'', involves the three explicitly depicted functions. Processing refers to activities that are performed in order to prepare the collection for review. This could be seen in the form of sorting, numbering and categorizing different forms of evidence. The manual review of evidence, can be regarded as someone looking at each document and making decisions on responsiveness, privilege and perhaps other issues which is often being referred as ''issue-coding'' (Webber and Oard, 2012).

According to Billard (2009), Webber and Oard (2012), contemporary review of evidence is mostly conducted with the assistance of technology meaning that the actual review will generally involve some human examination of documents, but it can also involve automatic classification. After the review of evidence, the actual analysis has to be done. Analysis in this context means control over the reviewing process: combining information seeking behavior or in other words content/metadata analysis (the analysis of what one wants) with formative evaluation or process analysis (the analysis of how well one is at finding what one wants). According to the EDRM-model website, usually one would expect to do an analysis after the review. Analysis entails finding key patterns, topics and people out of the reviewed evidence. However, the process of analysis can be implemented in different stages of the e-discovery process as well (https://www.edrm.net/resources/frameworks-and-standards/edrm-model/analysis/). Furthermore, the process of analysis must not be seen as a linear process, but as an iterative process where the research team continuously develops and revises its research strategy, in order to get to logical and useful information (see figure below).



Source: https://www.edrm.net/resources/frameworks-and-standards/edrm-model/analysis/

The fifth phase, production, involves the production of the reviewed and analyzed evidence into a human-readable format (Billard,2009). According to Webber and Oard (2012), production involves the delivery of responsive and non-privileged ESI to the requesting party, often accompanied by a log identifying any responsive and privileged ESI that has been withheld. In other words: all the gathered information being brought into a readable handheld in order to get to a better decision-making process.

4.1.4 Conclusion: The EDRM-model vs the traditional intelligence cycle

A first look at both models as the ways of processing intelligence, tells us that both entail a cyclical and iterative process: continuous adjustment of each phase during the research of a certain topic without an end. Both models share a lot of similarities based on the process of the initiation, collection, processing and dissemination of intelligence.

The planning and direction of intelligence efforts of the traditional intelligence cycle can be seen through EDRM-model as the combination of the phases of information management and the identification. Both entail the settlement of requirements, the assignment of tasks and the identification of information that is needed. The third phase of the EDRM-model is very similar to that of the traditional intelligence cycle: it involves the collection and preservation of intelligence that is deemed to be relevant. The fourth phase of the EDRM-model can be translated into the processing and analysis of raw intelligence phase of the traditional intelligence cycle. A first look would tell us that it would involve the same functions. However, if we look closely, it can be argued that the ''identification'' step from the EDRM-model already involves the functions of the processing of raw intelligence phase of the traditional intelligence cycle. Hence, when using the EDRM-model instead of

the traditional intelligence cycle, one enables himself to already validate the used sources on credibility and validity before the process of validation of the actual gathered intelligence is being practiced, when following the traditional intelligence cycle. This implies that for certain research topics, the EDRM-model enables organizations to work more efficient, given the fact of earlier detection of possible invalid sources and invalid information compared to the traditional intelligence cycle. Thus, it can be stated that in theory, the applied organizational process of processing intelligence of Bellingcat (in terms of checking the credibility and validity), with the use of the EDRM-model, is on many points similar to the traditional intelligence cycle what may indicate that the approach of Bellingcat towards these research questions are quite similar to that of the traditional intelligence cycle. However, the EDRM-model enabled Bellingcat to collect high quality intelligence faster, given the differences in early detection of possible invalid sources.

In the next section of this thesis, the report on the separatists' Buk will be analyzed in order to look if similar collection and analyzing methods are applied.

4.2 Sub question 2: *To what extent is Bellingcat able to use the same methods of collection and analysis compared to governmental intelligence organizations?*

4.2.1. Introduction

The report of Bellingcat (2014) analyses the preparations before the downing of MH17 and aftermath: the actions taken to remove the Buk trailer from the crime scene. The report contains three parts: the first part researches the part towards the actual downing of MH17. This part contains the preparations (the direction of movement of the Buk trailer and various actions taken to activate the Buk on Ukrainian territory). The second part addresses the origin of the Buk, by looking at its movement before crossing the Russian-Ukrainian border as a former part of the Russian 53rd Anti-Aircraft Missile Brigade, the people that moved it and their relation to the Buk and the aforementioned Russian Anti-Aircraft Missile Brigade. The third part addresses the movements and activities of vehicles that moved around the Buk in the aforementioned parts on July the 17th of 2014.

In order to make a statement whether Bellingcat uses similar methods of collection and analysis, the same format as the part of collection methods in the conceptual framework will be handled. This means that OSINT (and its subsequent parts IMINT and SOCMINT) and HUMINT will be analyzed separately. First, a brief introduction about OSINT, as a catch-all concept will be introduced. Second, the use of IMINT and SOCMINT analysis of the report will be analyzed in terms of breadth and depth. Third, the HUMINT analysis of the report will be analyzed in the same way.

4.2.2 OSINT

As already mentioned in the overview of the report (p.3), Bellingcat states that only open sources (OSINT) are used in the making of this report. The sources of the gathered evidence are collected through social media channels such as Facebook, YouTube, Twitter and Vkontakte (Russian social media website similar to Facebook), but also other traditional media such as magazines (Paris Match), newspapers (The Guardian and local newspapers) and websites. The vast majority of the gathered evidence entails photographs, videos, satellite images, tweets and posts from individuals on Twitter, Facebook, Yahoo and Vkontakte.

Traditional OSINT in the form of news articles from Paris Match, Buzzfeed, The Guardian and a local news report have been merely used as supplementary information whereas the other gathered intelligence from social media has been analyzed thoroughly by Bellingcat itself.

4.2.2.1 IMINT

Looking at the report and the different IMINT analysis techniques as mentioned in the conceptual framework, a couple of conclusions can be drawn. The report relies on extensive research of all the available imagery gathered from open sources. In this sense, the report can be placed into the third phase of IMINT production of Montgomery et. Al (1980) since the report combines photographs, videos and satellite images in order to identify the objects and their movements at specific times, locations and directions.

Section 1: The July 17 Buk

The photograph used on page 4 is an example of target identification/classification and delineation: the identification of the object as the Buk trailer and the identification of the area (the H21 motorway) what enabled Bellingcat to tell the direction (eastward direction of travel) of the moving object. After an inquiry with Paris Match, the time of the picture taken (around 11PM) could be verified by looking at shadow casts, which in turn, is a combination of delineation and measurement: the analysis of brightness and density in combination with the identification of the area looking at textures. The next image (p.5) shows a screenshot of a video that was posted on YouTube. Bellingcat (2014, p.6) stated that: ''*along H21 from the location in the Paris Match image. Using information provided with the video, it was possible to find the exact location the video was filmed, the H21 motorway running through Zuhres, and to show the Buk missile launcher continued to travel east*''. Again, target identification/classification in combination with geo-location (google maps) was made in order to verify the direction of movement of the convoy. On the photograph on page 6, the picture of the Buk trailer in a small town named Torez, Bellingcat stated: '' *It was again possible find the exact location the photograph was taken, and using shadows visible in the image it was estimated the time the photograph was taken was approximately 12:3''.* Using target identification/classification in combination with measurement and delineation enabled Bellingcat to identify the next step of the convoy.

The next photograph and video, analyzed on p.8, filmed a BUK moving on its own power. The Buk was identified (target identification/classification) as the Buk filmed and photographed in Torez and the precise location of the footage (Snizhne) was retrieved through geo-location. This geo-locating took place with the use of satellite images of the area provided through Google-street view. The location was analyzed by looking for obvious landmarks such as the road with trees in the middle, which is quite uncommon for the Snizhne area: '' *The obvious question is whether or not this is actually Snizhne, so the first thing to do is see if there's any obvious landmarks in the video*.'' (https://www.bellingcat.com/resources/case-studies/2014/07/17/geolocating-the-missile-launcher-linked-to-the-downing-of-mh17/). The analysis continues with the use of classification and enumeration of different characteristics of that certain area (differences in height, trees and houses), comparing the footage with the satellite imagery provided by google-street view. Furthermore, through the measurement of the shadow casts, Bellingcat was able to tell the time the footage was taken. As Bellingcat was able to tell the precise location of the taken footage, it was therefore also able to tell the direction of the moving Buk, which was towards the location of the crash site.

The last video (p.9), analyzed in the first section, is a video that was posted by the Ukrainian government on the 18th of July. It showed a Buk, back on the low-loader, missing one missile in the area of Luhansk.

Although the Russian government stated that the video was taken from Ukrainian controlled territory, Bellingcat was able to link the footage to the precise location, with the help of crowdsourced imagery: '' *A Luhansk local visited the place the video was reportedly filmed in Luhansk, and photographed the area, including objects that appeared in the video. It's clear that objects in the video match perfectly to the video''* (Bellingcat, 2014). By delineation (comparing the footage with the provided imagery), Bellingcat stated that it proved that the footage was taken from a town in a rebel-controlled area near the Russian border. The report goes on by analyzing footage of the low-loader truck that moved the Buk trailer in the beginning towards the crash site and after the actual downing of MH17, from the crash site to the rebel-controlled city of Luhansk. By comparing satellite footage of different days provided through Google-Earth (July 24th 2014 and the 9th of August 2014, Bellingcat was to tell that the trailer was moved during that period at least two times.

If we look at the first section of the report and the used Imagery analysis techniques, some conclusions can be drawn:

- The routinely conducts of Imagery analysis as been described by Kovarik (2011) are being practiced: the first section entails the detection, localization, recognition, identification, listing, comparison, interpretation and understanding of the involved imagery are part of the analysis as being described above.
- In this section, extensive use has been made of feature extraction, looking at the extent to which target identification / classification, measurement of objects and areas and delineation have been used in order to determine the origin and area of the footage.

Section 2: The June Convoy and "Buk 3x2"

This section analyses the movement of a convoy from the area of Kursk towards Ukrainian territory by analyzing a wide variety of open sources (photographs and videos) in order to determine the origin of the convoy that has been analyzed in section 1 that has been linked to the downing of MH17. The used sources include 16 videos that have been retrieved from Vktontakte, YouTube, Instagram and Odnoklassniki (Russian social media website). According to Bellingcat (2014), the exact location of each video could be retrieved. By comparing the distinct characteristics of the vehicles of the convoy of all videos (license plates, unit designation numbers and distinct traces of damage), the exact movement of the convoy from Kursk towards Millerovo (Russian town close to the Ukrainian border) could be tracked:

''*As the basis for the geolocation work, the previous videos from June were utilized both as reference material, as well as to give indications of a possible route which would narrow down the search area.*'' (https://www.bellingcat.com/news/2014/11/07/geolocated-june-buk-convoy-videos-in-russia/)
Bellingcat used a detailed measurement and calculation of the ''fingerprints'' (p.22),the side skirts of the Buk which are unique for every vehicle, on different videos from different days and comparing them, the similarity of the Buk trailer could be determined. Furthermore, the exact locations could be retrieved through detailed delineation (distinct characteristics of the area). This has been done for each video according to the article on the subject posted on their website (https://www.bellingcat.com/news/2014/11/07/geolocated-june-buk-convoy-videos-in-russia/).
Furthermore, as we can see on p.20, an imagery mosaic (overlapping photographs to construct a single picture) has been used in order to determine the similarity between the video from Paris Match (footage taken from Ukrainian territory) and footage taken from Russian territory of the Buk.

After reviewing the second section of the report, it can be stated that:

- looking at the many different IMINT analysis techniques (measurement, delineation, target identification/classification and creating imagery mosaics) high quality and detailed imagery analysis tactics have been used as been described by Diamond (2001) and Kovarik (2011)
- The focus of the second part in terms of IMINT analysis techniques lied on measurement of the side skirts of the Buk trailer combined with comparison (of plate numbers, unit designation numbers) and deep analysis of the similarities of the analyzed 16 videos and the delineation of the area of each video, in order to determine the direction of movement of the convoy.

Section three: The July Convoy

This section analyses footage taken of vehicles that were part of the same convoy as the Buk trailer, that has been linked to the downing of MH17 and have been filmed in the period after the downing of MH17. This footage is of interest, because it could link some vehicles to the 53rd Russian anti-aircraft brigade from Kursk. In this sense, the link could be established to Russian meddling into the Ukrainian conflict between Russian supported rebels and the Ukrainian government. This section includes footage (10 videos) taken from social media in the days of July 19th and 20th (a month after the downing of MH17). In order to determine whether these vehicles did appear on Ukrainian territory, the footage from the 10 videos is compared to the footage taken from Ukrainian territory, where license plates, unit designation numbers and other distinct features of the vehicles are compared in combination with photographs of soldiers that could be linked to the 53rd Russian anti-aircraft brigade from Kursk (photographs of Soldiers who take part in the convoy):

> *''Comparing the tarp-covered trailers, we can see an exact match to a July 19th video. It seems highly unlikely two identical convoys with exactly the same kind of vehicles, including the tarped loads, would have moved through the city 11 days apart, especially when no other footage from July 30th has been found…The final video of this convoy, number 11, provided no reference location, and was one of the more difficult ones to locate. One tool used was SunCalc, as likely time of the video filmed was known, so the shadows of the vehicles provided a clue about road orientation. Then, the matching road shapes were searched from the likely convoy route based on the June convoys movements, giving a match to the Olkhovatka. Finally, Street View was used to confirm the match.''*

*Source:(*https://www.bellingcat.com/news/uk-and-europe/2014/11/07/geolocated-july-buk-convoy-videos-in-russia/).

Just as in the former two sections, a combination of target identification /classification through the analysis of license plates and unit designation numbers and delineation techniques of the area of the footage, the actual movement of the convoy on Russian territory could be retrieved. By cross-referencing the different findings, from different perspectives and different analyzing techniques (SunCalc and IMINT feature extraction techniques), enabled Bellingcat to identify the same Buk trailer that has been filmed on Ukrainian territory.

Conclusion

The used imagery analysis methods and techniques, the results and subsequent conclusions point to an organized detailed analysis of the convoy, using IMINT as the primary data source, but combining this data with other sources (satellite imagery, SunCalc, locations retrieved from twitter posts and footage on YouTube), which can be related to the third phase of IMINT analysis from Montgomery et. Al (1980), in which systematic analysis of image material is carried out on the basis of three main pillars:

- Target identification/classification: through finding distinct similarities/marks of the vehicles that appear in the footage
- Delineation: by finding distinct characteristics of the environment that appear in the footage, cross-referencing and validating these characteristics with images retrieved from Google Earth/Street view, to determine the direction of movement combined into a map
- Measurement: the detailed measurement and calculation of the side skirts of the Buk trailers involved, in order to determine the authenticity of the trailer in each video

Thus, according to the findings, it can be stated that the actual IMINT research takes place in the third phase of IMINT analysis as posed by Montgomery et. Al (1980): a detailed analysis of the convoy in combination with the use of other sources. This means that the research cannot be fully attributed to the domain of intelligence, and thus, cannot be seen as the primary (but more secondary) practice of intelligence. However, the detailedness and the practiced techniques point at a sophisticated/professional use of IMINT analysis techniques which in turn, is similar to that of governmental intelligence agencies.

4.2.2.2 SOCMINT

Social network analysis

The report draws heavily upon intelligence gathered through social media channels with especially a focus on tweets from citizens that at that time lived in the specific area of interest and posts on Vkontakte (Russian counterpart of Facebook), since people from Ukraine and Russia are more familiar with Vkontakte than Western oriented Facebook. Of the 48 sources that have been used in the report, 20 sources are taken from Twitter, Vkontakte and Odnoklassniki.

In the first two sections of the report, tweets from eyewitnesses that were posted in the same area, date and time were being combined in order to reconstruct the movement of the Buk-trailer convoy which indicates to a light practice of Social network analysis, as being described in the conceptual framework: the practice to find the structure and topography of social networks in order provide an oversight of a dynamic and rapidly evolving situation. Examples of this practice can be found on page 6 and 7 and especially page 13, where footage has been placed onto a map to show the exact movement of the convoy. In the third section, another example of Social media network analysis can be found on page 26, where the movement of the convoy on Russian territory has been displayed on a map with added screenshots of the involved footage.

Manual analysis: ‘’netnography’’

The third section especially relies on the manual analysis or ‘’netnography’’ of the individual accounts that provided the imagery of vehicles that could have been part of the convoy that travelled through Ukrainian territory as well.

As being described in the conceptual framework, it often aims for depth over breadth in order to reveal and untangle the hidden, obscured, overlooked or contingent social significances, meanings and subjectivities experienced by individuals on social media. This in-depth analysis entails the analysis of videos and photographs of soldiers, photographed on, with or near vehicles. Comparing these different videos and photographs, posted on different dates and time, from different social media accounts have served three reasons:

- Establishing the link between the convoys that travelled through Russian territory in late June 2014, the separatist controlled area in Eastern Ukraine on the 17th of July 2014 and the convoy that travelled through Russian territory close to the Ukrainian border on the 19th and 20th of July 2014 by comparing vehicles and their distinct marks, plate and unit designation numbers
- To determine the direction of movement of the convoy
- To establish the origin of the convoy travelling through Russian territory had to be analyzed thoroughly. This means that the origin and motivation of the people behind the involved accounts needed to be traced. In this way, Bellingcat was able to find out that the persons behind the pictures from the late June convoy and the convoy of 19th and 20th of July, were in fact part of the 53rd Russian anti-aircraft brigade.

Solicited / 'crowd sourced' insight

According to Bartlett and Miller (2013), solicited or 'crowd sourced' insight refers to the practice of agencies to use social media to ask citizens or social media users for information directly. In the case of the Bellingcat report, this has happened twice in the search for the location of the Buk trailer filmed on the 17th of July 2014 after the downing of MH17 (p.8):

- The CEO of Bellingcat, Eliot Higgins tried to determine the exact location of the Buk trailer filmed, which was at the time of the investigation unclear. He decided to ask his followers: *''I shared the video with my Twitter followers, asking if anyone could find the area (crowd-sourcing these things can be useful), and quickly several people pointed to an area south of the center of Snizhne''* (https://www.bellingcat.com/resources/case-studies/2014/07/17/geolocating-the-missile-launcher-linked-to-the-downing-of-mh17/)

- With the help and advice of KoreanDefense.com to check a website with a collection of cameras, Bellingcat was able to identify the place as the town of Snizhne: *''A number of people have searched for matches between images in that area, and in the video. For example, KoreanDefense.com highlighted a website with a collection of cameras in the area being shared on the internet. All the cameras have now been shut down "by order of the government", but the preview images are still visible from before they were cut off…''* (Idem)

Conclusion

It can be stated that the report draws heavily upon human intelligence that is gathered through social media channels (Twitter, Vkontakte and Odnoklassniki). In order to secure this intelligence, the practices of social media network analysis, netnography and crowd sourcing have been used. The used SOCMINT techniques of social media network analysis, netnography and crowd sourcing and the absence of mathematical analysis indicate that Bellingcat has not the resources/techniques that are similar to that of governmental intelligence agencies. As been pointed out in the conceptual framework, this has positive and negative implications:

- The absence of (quantitative) mathematical techniques means that Bellingcat is not able to detect patterns of behavior within large groups and thus is not able to make any predictive claims on this matter. Which has, in turn, implications for the scope of the research (low reliability)
- The presence and focus on (qualitative) manual analysis techniques (social media network analysis and netnography) enables Bellingcat to detect early radicalization/civil unrest within smaller groups, meaning that Bellingcat is able to make claims and inferences within a small and delineated subject. This would indicate that the claims that have been made would at least be of high validity.

However, it seems that the SOCMINT analysis practiced, especially when looking at the part of netnography (the intensive investigation of the used social media accounts), lacks validation. As been stated by Omand, Bartlett and Miller (2013), gathered information through social media channels should be reviewed with great caution, since it is prone to contain misleading or distorting information: the recirculation of half-truths and mistakes. Wrong tweets by trolls or bots could have been picked up and used for the report. Given the fact that SOCMINT should be approached as the digital form of HUMINT, an extensive reviewing scheme like with HUMINT is missing. For example, on p. 10 of the report, Bellingcat tried to debunk the Russian statement on the Buk-trailer.

However, they did this with the help of a HUMINT source (Bellingcat,2014,p.10 & (https://www.bellingcat.com/news/uk-and-europe/2014/07/24/caught-in-a-lie-compelling-evidence-russia-lied-about-the-buk-linked-to-mh17/) , which in turn, has not been validated at all. This does not improve their claims. On the other hand, it seems that Bellingcat has tried to minimize the lack of validation through extensive cross-referencing techniques by practicing IMINT analysis and geo-locating techniques. In this sense, the social media channels could be seen as the primary source of the gathered intelligence. This intelligence, in turn, is mostly imagery (photographs and videos). However, the lack of source validation, which is crucial for SOCMINT analysis, is absent. This has serious ramifications for the credibility of the report. Thus, it can be stated that although many elements of qualitative SOCMINT collection and analysis techniques are used that are similar to that of governmental intelligence agencies, Bellingcat cannot be placed into the realm of intelligence agencies, given the lack of a strong validation strategy, which is essential in managing and processing social media intelligence.

4.2.3 HUMINT

HUMINT

As earlier mentioned in the conceptual framework, HUMINT is intelligence obtained by people that is mostly collected from information that is available in the open domain (Herman,1996; Johnson,2010). Looking at the report, it can be stated that the report entails one example of traditional HUMINT, where a Luhansk resident photographed the area and has send the pictures to Bellingcat in order to debunk the statement of the Russian government (https://www.bellingcat.com/news/uk-and-europe/2014/07/24/caught-in-a-lie-compelling-evidence-russia-lied-about-the-buk-linked-to-mh17/). But, verification of the sources did not take place, or at least, was not mentioned (Bellingcat,2014, p.10).

Conclusion

Given the fact that HUMINT sources have a reputation of unreliable information, or at least are subject to human frailties, the credibility and validity of the HUMINT sources cannot be defined. Therefore, it can be concluded that on the base HUMINT collection, analysis and verification techniques, Bellingcat cannot be regarded to the domain of intelligence services, who have traditionally a strong validation scheme for HUMINT and its accompanied frailties.

4.2.4 Conclusion

This section of the thesis addressed the question to what extent Bellingcat is similar to governmental intelligence organizations, in their methods of collection and analysis. After reviewing the different types of intelligence (HUMINT, OSINT and its subsequent parts SOCMINT and IMINT), the following conclusions can be drawn:

Present characteristics of an intelligence organization

- Bellingcat's extensive use of OSINT: a characteristic of a well-developed intelligence organization is the extensive use of OSINT, accompanied with highly differentiated analysis techniques that are being practiced in the MH17 report.
- Bellingcat's professional (detailed) and organized IMINT analysis, using different techniques (target identification, delineation and measurement) and cross-referencing
- Strong qualitative SOCMINT analysis, which enabled Bellingcat to detect and make inferences about civil unrest/radicalization
- Extensive triangulation in order to minimize the lack of source validation

Absent characteristics of an intelligence organization

- The absence of source validation (for HUMINT and SOCMINT) which is crucial to the credibility of the research given the insecure nature of the intelligence
- The absence of quantitative collection methods and analysis, which is the primary focus of intelligence organizations
- Third phase IMINT analysis, resulting in the report to be more explanatory, while intelligence organizations are focused on predictive analysis

The characteristics that have been pointed out tell us something about to what extent Bellingcat is similar to governmental intelligence organizations when looking at methods of collection and analysis. The fact that Bellingcat lacks the resources/techniques and or capacity in the collection of intelligence (for example the lack of quantitative collection methods), forces Bellingcat to limit itself to pure OSINT analysis. The OSINT analysis and especially the subsequent IMINT and qualitative SOCMINT analysis are the strongpoints of the research. However, OSINT analysis requires an extensive validation strategy compared to intelligence obtained from more covert sources. The lack of source validation remains a big problem for the credibility of the report and the claims being made. Triangulation and cross-referencing have been practiced in order to validate the obtained intelligence.

Thus, Bellingcat is in their limited position (of available resources and techniques) able to analyze the obtained OSINT in a professional way that is similar to governmental intelligence organizations, but lacks the source validation.

However, this is a self-fulfilling prophecy: the missing techniques and resources that earlier limited Bellingcat to OSINT research, now require a comprehensive validation strategy, where resources and techniques in turn, are needed to handle these strategies. This is in contradiction with the findings from chapter 4.1: In theory, the EDRM model should enable one to detect possible invalid sources at an earlier stage than the traditional intelligence cycle. This means that when the EDRM model is followed, the credibility and validity of the sources would be assessed at an earlier stage. However, according to the findings of chapter 4.2, the validation of the sources are at some points insufficient (SOCMINT validation) and at other points absent (HUMINT source, p.10). Thus, for the collection methods and analysis of HUMINT and SOCMINT it can be claimed that the identification phase of the EDRM model has not been performed properly and subsequently the source validation of HUMINT and SOCMINT is absent. Therefore, Bellingcat cannot be placed into the realm of intelligence services, when looking at the SOCMINT and HUMINT analysis. The practiced cross-referencing/triangulation technique in the IMINT analysis, can be seen as professional manner of source validation. Therefore, when looking at the IMINT analysis, Bellingcat shows similarities with governmental intelligence organizations and can be placed into the realm of intelligence services.

4.3 Sub question 3: *To what extent is Bellingcat able to gather the same intelligence (overt and covert) in time and place compared to governmental intelligence organizations?*

As earlier mentioned in the conceptual framework, the authors of the suspicious Signs-model (SSM) argue that collecting information from historical files (derived from open sources) at times of the Suspicious signs phases Rumbling and Work-up process is very difficult, given the fact that these cases usually are not seen as important enough for the media and thus be reported. This section examines the extent to which Bellingcat was in fact able to uncover these phases. The analysis has been structured in the following way: The report will be analyzed on the basis of the phases Trigger, Rumbling and Work-up process, the situation wherein the phase took place, the characteristics or ''signs'' of that phase and the origin of the intelligence. Given the fact that the Suspicious signs model entails an iterative process with a very delicate balance between the conviction that something has to happen, the actual (Trigger) and the first premature forms of action (Rumbling), the decision has been made to include the Trigger phase into the analysis. Although this phase entails mostly overt intelligence and the others, according to Rademaker et. Al (2006), more covert intelligence. This can be justified, since each phase does not exclude the other (the aforementioned iterative process). However, the focus of the report is on the Rumbling, Work-up and Aftermath phase. This means that the origin of intelligence cannot be founded for the trigger phase. At the end, the newly added phase, Aftermath, will be discussed, followed by the conclusion.

4.3.1 Trigger phase

The Trigger phase entails a situation where an actor or multiple actors create a conviction that action must be undertaken. Governmental/political decisions and violent actions are examples that can be noticed through behavioral science, profiling of groups and thereby mapping types of groups or individuals that trigger on the occasions.

Examples of triggers are: inspirators (individuals or groups that take a stance and plea for action), governmental (political) decisions that lead to commotion, violent actions and / or public statements during the Work-up process that lead to persons or groups also wanting to manifest themselves. Trends with relevance to the Trigger phase are a hardening relationship between the citizen and the state and a rise in politically motivated activism (Rademaker et. Al, 2006).

The authors state that behavioral science analysis and profiling of groups and individuals is needed. These results must be matched with known risk groups and individuals. If we translate these premises into the case and apply them on the Bellingcat report, the following can be concluded:

Background and Suspicious signs

In December 2013, the Ukrainian revolution or ''Euromadain'' was taking place, which was a civil revolution against the Russian oriented government in order to ''Westernize'' the country and to strengthen the ties with the West (Kulyk,2016). Protests and governmental reaction to the protests intensified, culminating on February 18 where the bloodiest event took place, where the government forces killed 88 people during a protest on the Maidan-square in Kyiv (Shveda & Ho Park,2015).

- Governmental/political decisions that have led to commotion (the Governmental decision end the demonstration with a high number of casualties and the subsequent intensified demonstrations that have made the sitting president to leave the country)

4.3.2 Rumbling phase

The Rumbling phase entails the first premature forms of action. This means that certain developments on a political/societal level encourage the conviction (of a group) of the trigger phase to develop into a situation where a group bears the conviction that something has to happen. This often entails the entry of the group and/or another actor to the stage and small (political) actions are undertaken. The authors state that trend-analysis on media expressions, efficient tracking and analysis of open sources and analysis of data traffic is needed to identify patterns. HUMINT and SIGINT can contribute to this. If we translate these premises into the case and apply them on the Bellingcat report, the following can be concluded:

Background and Suspicious signs

In February 2014, the revolution was still going when president Yanukovich decided to leave the country, which meant new elections had to take place. In May 2014, the presidential election took place while Russia annexed Crimea from Ukraine and pro-Russian terrorists in Donetsk and Luhansk regions were trying to ban the election altogether (Shveda & Ho Park, p. 90). When looking at the given situation, some suspicious signs could be extracted:

- The entry of Russia as an actor in the conflict by annexing Crimea
- Pro-Russian terrorists banning the Ukrainian elections in the Donetsk and Luhansk regions
- Military movement around the eastern border of Ukraine
- Media reports of moving convoys on Russian territory to strengthen border controls

Origin of the intelligence

The second part of the Bellingcat investigation, on the origin of the Buk trailer, analyses intelligence that has been disseminated in the month of June 2014. It analyses the movement of the Buk trailer from Kursk (Russian city near the Ukrainian border) towards the Ukrainian border, officially as part of a military exercise (p.14). This section involves the analysis of 16 videos posted on social media sites including Vkontakte, YouTube, Instagram and Odnoklassniki.

According to Bellingcat (2014), these footage shows that the 53rd Brigade's convoy was moving from Kursk to Millerovo between June 23rd and June 25th. Given the trigger of the entry of a new actor (Russia), the governmental decisions that have led to commotion and violent actions of the Pro-Russian terrorists who discard the Ukrainian government as their sovereign and the same period wherein the footage/intelligence has been produced that has been analyzed in section 2 of the Bellingcat report, one can assume that this section involves the analysis of the Trigger phase. Furthermore, as Bellingcat states, it was also possible to find a local news report about the convoy travelling in the region, to strengthen the border controls. These findings reject the assumptions of Rademaker et. Al (2006): The assumption that open source intelligence is difficult to obtain during the Rumbling phase given the fact that the media does not report these cases at all. Furthermore, Bellingcat proves that open source intelligence is no longer solely confined to the traditional mediums, by extracting footage from social media channels and other open sources such as Google earth, which in turn enabled Bellingcat to make to some extent statements on the movement of the convoy.

4.3.2 Working-up Phase

Background and suspicious signs

During the working-up phase, the emphasis lies on signs that contribute to the process towards violent action. Given the fact that the Suspicious signs model entails a iterative process, earlier suspicious signs have to be taken into account: individuals or groups have the conviction that something has to happen, another actor entered the stage, intensifying fights between pro-Russian rebels and the Ukrainian government, Russian military movement around the eastern border of Ukraine and media reports of a convoy that is moving towards the Russo-Ukrainian border as a sign of premature action show a process that is slowly stepping-up towards the working-up process: the actual preparations that are being made for violent action. According to Rademaker et. Al (2006) suspicious signs of the working-up process could be the concentration of resources, recruiting, training, reconnaissance and planning of violent actions.

These signs could be noticed through tracking suspicious persons, travel patterns, contacts and meetings and the use of infrastructure. If we translate these premises into the case and apply them on the Bellingcat report, the following can be concluded:

- Breakthrough in intent: the Russian convoy being filmed in the eastern Ukrainian region which indicates the process has stepped up from premature action towards actual support of the pro-Russian rebels and thus can be noticed as a suspicious sign of the working-up process
- The travel pattern suggests that this military equipment has been send from Russia to support the pro-Russian rebels in the east in the city of Donetsk

Origin of intelligence

The first section of the report analyses photographs (3), videos (3) accompanied by tweets (3) and posts on Vkontakte (2) that has been made or have been posted on social media on the 17th of July 2014. The section analyses the footage of the Buk trailer in Donetsk, Zuhres, Shakhtarsk, Torez and Shnizhne (in order of time), to determine the direction of movement of the Buk trailer. Although one cannot know when or where the actual violent action will take place, one can assume that given the suspicious signs and developments of the foregoing phases accompanied with the new developments of the travel pattern of the Buk trailer and the fact that this Buk trailer was filmed on Ukrainian soil, the related footage can be placed in the working-up phase. Thus, it can be stated that next to the Trigger and Rumbling phases, Bellingcat proved that through decent IMINT analysis retrieved with the use of SOCMINT techniques, open source intelligence (OSINT) can be found and used for the working-up phase.

4.3.3 Aftermath

Since the suspicious signs model stops after the actual violent action, the choice has been made to add a new phase, Aftermath, accompanied with different suspicious signs, since this could have possible benefits for the criminal investigation onwards in which intelligence services often remain involved.

The Aftermath phase entails the suspicious signs of the foregoing phases, but instead of a process that is stepping up, these suspicious signs do rapidly step down and/or disappear. In other words: information (evidence) that is available after the violent action, rapidly evolves from overt towards covert information, before disappearing.

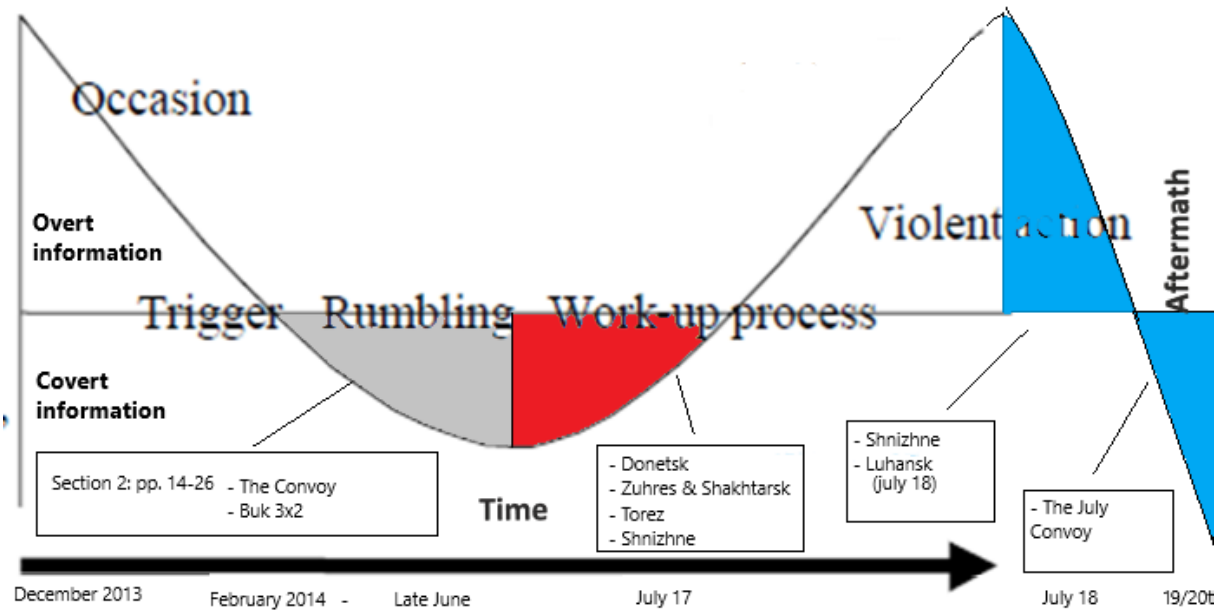
The following suspicious signs can be identified:

- Destruction of evidence (short-term) (Trouw, 2014)
- Hiding of evidence (short-term) (Trouw, 2014)
- Travel patterns that suggest a military movement out of Ukraine (short-term) (Bellingcat, 2014)
- Declining media reports (short-term) (Bellingcat, 2014)
- Russia stepping down in supporting pro-Russian rebels (long-term)

Already in the first section, Bellingcat was able to identify footage that was taken after the downing on the 18th of July filming the Buk trailer in the city of Luhansk driving eastern direction. In the third section, footage (containing 10 videos of the Buk trailer and other vehicles that were part of the same convoy) was analyzed dating from the 19th and 20th of July 2014 and filmed again on Russian territory. Most of the footage (10 videos) was retrieved from Vkontakte and Odnoklassniki.

4.3.4 Suspicious signs model and figure

After reviewing the report, the following conclusions regarding the figure of the Suspicious signs model can be drawn:



This figure, which was originally used for the visual representation of the Suspicious signs model, has been adjusted and supplemented with the findings from the report. As can be seen in the figure, the Suspicious signs model assumes that the Rumbling and Work up phases mainly contain covert intelligence. The analysis of the report, using the Suspicious signs model, showed that for each phase the characteristics and the suspicious signs were identified using OSINT. It can be concluded from this that the assumption of the model, that mainly covert techniques and intelligence must be used to collect covert intelligence, and thus the implicit assumption that only intelligence and investigation services have these possibilities, can be rejected. Bellingcat has proved that, with the use of open source intelligence, each phase can be detected. The suspicious signs of each phase have also been discovered in a detailed way. Given the sophisticated way of analysis and how the ''dots'' have been connected and the high degree of detail of which the Rumbling and Work-up phase and subsequently the depth of each phase is being covered, it can be concluded that Bellingcat is on these points very similar to governmental intelligence organizations and the way they are able to analyze the collected intelligence with the help of the Suspicious signs model by using only Open Source Intelligence (OSINT).

Furthermore, the original model assumes that after the actual violent action, the suspicious signs added together at each stage should have disappeared immediately. This is an incorrect assumption. In addition to preventing violent acts, intelligence and investigation services are tasked with detecting, arresting and surrendering terrorists to the judiciary. Bellingcat has proved that with only OSINT analysis, the process towards the downing of MH17 can be described. Perhaps even more important, is the fact that Bellingcat was able to describe and analyze the process after the downing of MH17 (Aftermath phase) in a professional and detailed manner.

This offers important theoretical and practical leads for intelligence services and investigative services in the use of OSINT and in particular Social media intelligence (both monitoring and therefore preventive in nature, as well as investigative and explanatory) in order to be able to follow the perpetrators in their path of destroying evidence and escape in the Aftermath phase.

4.3.5 Conclusion

Thus, after reviewing the report with the help of the Suspicious signs model and the results of the report and the analysis, the following can be concluded:

- Bellingcat is able to cover each covert (Rumbling and Work-up) phase of the Suspicious signs model in high detail (depth) placing them in the realm of intelligence organizations.
- Bellingcat showed that with a strong and sophisticated analysis, it has been able to uncover a new phase: the Aftermath phase, which is crucial in detecting and trying criminals/terrorists
- The assumption of the Suspicious signs model that the Rumbling and Work-up phase are need to be uncovered by covert techniques can be rejected, since Bellingcat has been able to uncover these phases using OSINT.
- The implication of the aforementioned assumption of the Suspicious signs model, that the Rumbling and Work-up phases can only be covered by means of covert techniques and therefore only intelligence organizations are capable of doing so, can also be rejected.
- Bellingcat has demonstrated that the Suspicious signs model is limited in its assumption that suspicious signs are no longer present after the violent action, given that it has demonstrated that suspicious signs can be detected even after the actual violent action through thorough OSINT (and in particular qualitative SOCMINT) analysis.

5.0 Conclusion

This thesis addressed the research question: '' *What are the similarities in the way of working between Bellingcat as a private investigative journalist group and governmental intelligence organizations, seen through the different stages of the intelligence cycle (organizational process), the collection of overt and covert information through the suspicious signs-model (sources of information) and collection methods (activities), illustrated by the case of MH17 and the report on the source of the separatists' buk?''*.

In this thesis, the following concepts have been used to make claims about the extent to which Bellingcat is similar to governmental intelligence organizations:

- The traditional intelligence cycle: the organizational process of processing intelligence
- The different intelligence collection methods and analysis
- The Suspicious signs model: the nature of the collected information and the subsequent analysis

''To what extent is Bellingcat similar to governmental intelligence organizations when looking at the organizational process of the intelligence gathering process?''

When looking at the organizational process of the processing of intelligence, the comparison that has been made between the traditional intelligence cycle (what resembles the basic process of intelligence services in processing intelligence) and the EDRM-model that is being practiced in the processing of intelligence by Bellingcat, it can be stated that these models share many similarities. The collection, processing and dissemination phases, which are the main pillars of the traditional intelligence cycle can also be found in the EDRM model. Thus, the claim can be made that the EDRM model, in theory, is suited for the processing of collected intelligence. If we look at the level of depth that has been used by Bellingcat, it can be claimed that each phase has been addressed: intelligence has been collected, processed and disseminated in the form of the report. This indicates that the approach of Bellingcat towards the gathering and processing of intelligence are in some way similar to that of governmental intelligence services. In theory, the EDRM-model enables one to collect high quality intelligence faster, given the differences in early detection and possible invalid sources. However, when looking at the results of the analysis, and thus in a practical sense, Bellingcat did not use this advantage in their report, given the lack of validation. The commonly used sources do not provide an accurate analysis of reliability. This means that overall, the same process has been followed. But, at the same time, it can be stated that the level of depth, practiced by Bellingcat, remains superficial. Thus, in theory, it can be stated that Bellingcat and governmental intelligence services share many similarities. In a practical sense however, especially when looking at the validation, it can be stated they do not share any.

To what extent is Bellingcat able to use the same methods of collection and analysis compared to governmental intelligence organizations?

The second section of the analysis, addressed the extent to which Bellingcat has used the same types of collection methods and analysis compared to governmental intelligence organizations. The analysis of the report has showed that each of the collection method (HUMINT, SOCMINT and IMINT) have been used. However, the extent and depth of use varies per collection method. After reviewing the report, it can be concluded that the report has a strong and detailed in-depth analysis of the collected IMINT, where professional methods of analysis have been used, that are similar to that of governmental intelligence organizations. However, the detailed analysis of IMINT indicates a third phase IMINT analysis, which means that the report is more explanatory than predictive.

Furthermore, Bellingcat practices a sophisticated way of triangulation/cross-referencing, in their IMINT research, to minimize and compensate their lack of source validation. On the one hand, the practice of triangulation/cross-referencing hints towards a professional way to cope with limited research tools and therefore be regarded as a characteristic similar to that of governmental intelligence organizations. On the other hand, it can be stated that the lack of source validation remains a big problem throughout the report and has implications for the credibility of their findings.

Next to the IMINT analysis, it can be concluded that although the SOCMINT analysis lacks source validation and quantitative forms of analysis, a professional qualitative assessment of SOCMINT in the form of manual analysis has been practiced. Given that, it can be claimed that when looking at the qualitative SOCMINT analysis, Bellingcat is able to reach the same level as that of governmental intelligence organizations. However, the lack of source validation is a limiting factor. Last, the practiced level of HUMINT, in amount and the level of depth, is almost not worth mentioning. Only one HUMINT source has been used and in the analysis. This source has not been validated, although this is crucial in using HUMINT with its accompanied frailties and its susceptibility to deception. Therefore, it can be claimed that when looking at the practiced HUMINT, Bellingcat is not similar to governmental intelligence agencies.

To what extent is Bellingcat able to gather the same intelligence (overt and covert) in time and place compared to governmental intelligence organizations?

The third part of the thesis addressed the question to what extent Bellingcat is able to collect the same intelligence compared to governmental intelligence organizations, when looking at the nature of the gathered intelligence. The main focus of the section lied on the analysis of the Rumbling, Work-up and the newly added aftermath phase. The analysis has showed that all phases are being covered by Bellingcat. Bellingcat proved that with only OSINT research/investigation, covert information could be retrieved. The degree of depth is worth mentioning, given the fact that Bellingcat has only used OSINT in their analysis and they were able to make strong claims about phases that are presumed to entail mostly covert information (Rumbling and Work-up phase). The degree of the in-depth analysis of the Aftermath phase indicates that the same level of detail in the analysis is used as that of governmental intelligence organizations, and maybe even beyond. This has implications for the Suspicious signs model, given the assumption within the model that covert information needs covert collection methods. Furthermore, it is possible to reject the implicit assumption within the Suspicious signs model that only governmental intelligence organizations are capable of uncovering covert information. It has also shown that the model is too limited: after the violent action, not everything stops at once, but the suspicious signs decrease at the same pace as they rose before the violent action. This offers theoretical and practical leads for intelligence services in the use of OSINT and in particular the analysis of Social media intelligence in monitoring civil unrest/radicalization and the further examination of the newly introduced Aftermath phase, which could be of help for authorities in tracking down criminals/terrorists after the violent action.

Interrelationships

The organizational process of processing intelligence, the way intelligence has been collected and the nature of the collected intelligence cannot be viewed apart from each other. This is simply because of the fact that these parts more or less are related to each other. In this part, the interrelationships between the concepts and subsequent findings, will be discussed.

The section that addressed the methods of collection and analysis (4.3), pointed out that Bellingcat limits itself to pure OSINT and HUMINT. Although we do not know what the exact capabilities of Bellingcat are in terms of sources and techniques, we can assume that they are less than the capabilities of governmental intelligence organizations. As stated in the conceptual framework, HUMINT and OSINT (and subsequently SOCMINT and IMINT), given their insecure nature in terms of credibility and validity, require an extensive validation strategy. This, in turn, requires high developed techniques and much resources in terms of time and finances.

It can be assumed that given the resources that are present, Bellingcat has made the choice to stick to OSINT analysis, because it is a low-cost source with high return in terms of intelligence. This seems like a self-fulfilling prophecy: the lack of resources and capabilities, forces Bellingcat to practice only OSINT analysis. However, OSINT analysis requires an extensive validation strategy, which can only be practiced when one has the capabilities and resources to follow this validation strategy. In theory, the EDRM model (4.1) provides a good low-cost validation strategy for the used sources. However, according to the findings of chapter 4.2, the validation of some sources is insufficient and at some points absent. Thus, as earlier mentioned, the identification phase of the EDRM model would be a solution, but has not been practiced properly.

However, the benefits of the professional OSINT analysis do have a positive effect on the part of the Suspicious signs model. It enabled Bellingcat to cover the Rumbling and Work-up phase, which initially were deemed to be the field of governmental intelligence organizations (given their covert nature). Although the claims cannot be regarded as fully credible or valid, the speed with which Bellingcat has come to coherent claims is astonishing (less than 3 months after the crash), which can be explained by the organizational process (EDRM model) and the strong/detailed IMINT and qualitative SOCMINT analysis. Furthermore, Bellingcat was able to uncover a new phase, the Aftermath phase, which can be regarded as a great contribution of OSINT analysis to the Suspicious signs model.

Overall conclusion

Overall, it can be concluded that Bellingcat and governmental intelligence organizations do share many similarities but also differ on many aspects: The traditional intelligence cycle and the EDRM model are in theory very similar, which indicates the same organizational attitude towards intelligence processing. However, in a practical sense, both organizations do differ in terms of source validation. The use of different collection methods and analysis by Bellingcat compared to governmental intelligence organizations is limited to IMINT and qualitative SOCMINT compared to a broad use of different collection methods and analysis of governmental intelligence organizations, but of a high-quality level that is comparable to that of the traditional intelligence services. Furthermore, the use of different collection methods and analysis by Bellingcat compared to governmental intelligence organizations is limited to IMINT and qualitative SOCMINT, compared to a broad use of different collection methods and analysis of governmental intelligence organizations. But the used collection methods IMINT and qualitative SOCMINT are of a high-quality level, that is comparable to that of the traditional intelligence services. Another important distinction between these two types of organizations is that Bellingcats' report is of an explanatory nature, which contradicts with the predictive nature of an intelligence organization. This will be further elaborated in the Discussion section (5.1).

5.1 Discussion

The current research complements existing literature on investigative journalist groups and their relationship (similarities) to governmental intelligence organizations because former studies have not incorporated Bellingcat and the Suspicious signs model into their analysis. On the basis of this investigation, intelligence services may consider to install an extensive Social Media monitoring/ detection system in order to prevent radicalization and civil unrest, given the fact that the vast majority of information (on these topics) is available from public open sources.

However, this research has a number of limitations: The amount of scientific literature on the work of intelligence services is very thin. This is, of course, due to the fact that the work that intelligence agencies perform must often remain non-disclosed. It should be taken into account that this study focused exclusively on Bellingcat and the MH17 report, and conclusions were drawn on the basis of the results of the report. This means that the results are valid, but these results are only valid for the Bellingcat situation and the case MH17, and are therefore not necessarily replicable and or applicable to other research groups.

Explanatory vs prognostic research

The question can be raised whether this investigation by Bellingcat actually concerns an intelligence investigation. In some parts of the report, professional analysis techniques that can be related to intelligence organizations are indeed used, but what makes the investigation a criminal investigation and thus an explanatory investigation is that the investigation took place after the disaster. However, the sources that are used, existed before the downing of MH17. This means that the information was there, but not yet known to the authorities involved. This means that the report is investigative of nature, but when we take the organizational process of processing intelligence, the different collection methods and analysis and the nature of the collected information (overt and covert) into account, it can be stated that it has many elements of an intelligence investigation.

Literature

Bellingcat. (2014). *Origin of the Separatists' Buk: A Bellingcat Investigation.* Retrieved from https://www.bellingcat.com/wp-content/uploads/2014/11/Origin-of-the-Separatists-Buk-A-Bellingcat-Investigation1.pdf

Best, C. (2008). Open source intelligence. *F. Fogelman-Soulié, Mining Massive Data Sets for Security: Advances in Data Mining, Search, Social Networks and Text Mining, and Their Applications to Security*, 331-343.

Burke, C. (2007). Freeing knowledge, telling secrets: Open source intelligence and development. *CEWCES Research Papers*, (11), 18.

Biermann, J. (2004). A Knowledge-Based Approach to Information Fusion for the Support of Military Intelligence. Research establishment for applied sciences Wachtberg-Werhoven (Germany) Ergonomics/Information Sys.

Billard, D. (2009, January). An extended model for e-discovery operations. In *IFIP International Conference on Digital Forensics* (pp. 277-287). Springer, Berlin, Heidelberg.

Brady, H. E., & Collier, D. (Eds.). (2010). *Rethinking social inquiry: Diverse tools, shared standards*. Rowman & Littlefield Publishers.

Bryman, A. (2016). *Social research methods*. Oxford university press.

CTIVD. (2015). *Toezichtsrapport naar aanleiding van de crash van vlucht MH17* (43). Retrieved from https://www.ctivd.nl/documenten/rapporten/2015/10/13/rapport-mh17

Collier, D. (2011). Understanding process tracing. *PS: Political Science & Politics*, *44*(4), 823-830.

Corps, U. M. (2002). Imagery Intelligence. Washington DC.

Degaut, M. (2016). Spies and policymakers: Intelligence in the information age. *Intelligence and National Security*, *31*(4), 509-531.

Diamond, J. M. (2001). Re-examining problems and prospects in US imagery intelligence. *International Journal of Intelligence and CounterIntelligence*, *14*(1), 1-24.

Dillon, P. J. (1998). *A Theory for Human Intelligence Operations*. ARMY WAR COLL CARLISLE BARRACKS PA.

Fingar, T. (2012). A guide to all-source analysis. *The Intelligencer. Journal of US Intelligence Studies. Association of Former Intelligence Officers*, *19*.

Herman, M. (1996). *Intelligence Power in Peace and War*. Cambridge University Press.

Hribar, G., Podbregar, I., & Ivanuša, T. (2014). OSINT: a "grey zone"?. *International Journal of Intelligence and CounterIntelligence*, *27*(3), 529-549.

Hulnick, A. S. (2006). What's wrong with the Intelligence Cycle. *Intelligence and national Security*, *21*(6), 959-979.

Ilyuk, Y. (2019). Journalistic Investigations in the Digital Age of Post-Truth Politics: the Analysis of Bellingcat's Research Approaches Used for the (Re) construction of the MH17 case. *Perekrestki*, (1), 56-78.

Irwin, D., & Mandel, D. R. (2019). Improving information evaluation for intelligence production. *Intelligence and National Security*, *34*(4), 503-525.

Johnson, L. K. (Ed.). (2007). Handbook of intelligence studies. Routledge.

Kovařík, V. (2011). *Imagery Intelligence (IMINT)*. Univerzita obrany.

Lehren, A. W. (2018). The Rise of Investigative Data Journalism. In *Digital Investigative Journalism* (pp. 9-17). Palgrave Macmillan, Cham.

Marrin, S. (2017). Understanding and improving intelligence analysis by learning from other disciplines. *Intelligence and National Security*, *32*(5), 539-547.

Montgomery, C. A. (1979). *Imagery Intelligence (IMINT) Production Model* (Vol. 1210). US Army Research Institute for the Behavioral and Social Sciences.

NATO (2001) NATO Open Source Intelligence Handbook. New York.

NCTV (2019) Nationale veiligheidsstrategie 2019. Den Haag.

Noordegraaf, M., Schiffelers, M. J., Geuijen, K., Morree, P. D., Pekelder, J., & Leferink, E. (2018). Op weg naar een Weerbare Open Samenleving. Universiteit Utrecht-Departement Bestuurs-en Organisatiewetenschap (USBO).

Oard, D. W., & Webber, W. (2013). Information retrieval for e-discovery. *Information Retrieval*, *7*(2-3), 99-237.

Odom, W. E. (2008). Intelligence analysis. *Intelligence and National Security*, *23*(3), 316-332.

Omand, D., Bartlett, J., & Miller, C. (2012). Introducing social media intelligence (SOCMINT). *Intelligence and National Security*, *27*(6), 801-823.

Omand, D., Miller, C., & Bartlett, J. (2014). Towards the discipline of social media intelligence. In *Open Source Intelligence in the Twenty-First Century* (pp. 24-43). Palgrave Macmillan, London.

Omand, D., Bartlett, J., & Miller, C. (2012). Introducing social media intelligence (SOCMINT). *Intelligence and National Security*, *27*(6), 801-823.

Rademaker et. Al (2006) *Denk- en datamodel Suspicious Signs*. Clingendael: Den Haag

Richelson, J. T. (2015). The US intelligence community. Hachette UK.

Shveda, Y., & Park, J. H. (2016). Ukraine's revolution of dignity: The dynamics of Euromaidan. *Journal of Eurasian Studies*, *7*(1), 85-91.

Steele, R. D. (2007). Open source intelligence. *Handbook of intelligence studies*, *42*(5), 129-147.

Stottlemyre, S. A. (2015). HUMINT, OSINT, or something new? Defining crowdsourced intelligence. *International Journal of Intelligence and CounterIntelligence*, *28*(3), 578-589.

Thibault, G., Gareau, L. M., & Le May, F. (2007, July). Intelligence collation in asymmetric conflict: A canadian armed forces perspective. In 2007 10th International Conference on Information Fusion (pp. 1-8). IEEE.

Toler, A. (2018). Crowdsourced and Patriotic Digital Forensics in the Ukrainian Conflict. In *Digital Investigative Journalism* (pp. 203-215). Palgrave Macmillan, Cham.

Websites

Bellingcat (2014) Geolocating the missile launcher linked to the downing of mh 17. Retrieved on March 22, 2020 from: https://www.bellingcat.com/resources/case-studies/2014/07/17/geolocating-the-missile-launcher-linked-to-the-downing-of-mh17/

Bellingcat (2014) Geolocated July buk convoy videos in Russia. Retrieved on March 22,2020 from: https://www.bellingcat.com/news/uk-and-europe/2014/11/07/geolocated-july-buk-convoy-videos-in-russia/

Bellingcat (2014) Caught in a lie compelling evidence Russia lied about the buk linked to MH17. Retrieved on March 25, 2020 from: https://www.bellingcat.com/news/uk-and-europe/2014/07/24/caught-in-a-lie-compelling-evidence-russia-lied-about-the-buk-linked-to-mh17/

Bellingcat (2019) Policy plan. The Hague retrieved from: https://www.bellingcat.com/app/uploads/2020/06/Bellingcat-Policy-Plan-2019-2021.pdf

De Volkskrant. (2014, July 17). Crash MH17, dit zijn de feiten. Retrieved March 6, 2020, from https://www.volkskrant.nl/nieuws-achtergrond/crash-mh17-dit-zijn-de-feiten~b765cef9/

De Volkskrant. (2014, August 7). Morgen keren eerste 135 experts terug in Nederland. Retrieved March 6, 2020, from https://www.volkskrant.nl/nieuws-achtergrond/morgen-keren-eerste-135-experts-terug-in-nederland~bed11f86/

De Volkskrant. (2015, January 6). Onderzoek naar kennis AIVD en MIVD over veiligheid Oekraïne. Retrieved March 9, 2020, from https://www.volkskrant.nl/nieuws-achtergrond/onderzoek-naar-kennis-aivd-en-mivd-over-veiligheid-oekraine~b31a9b76/

https://www.edrm.net/resources/frameworks-and-standards/edrm-model/identification/

Modderkolk, H. (2015, February 9). "AIVD zat ten tijde van MH17 niet in Kiev." Retrieved March 9, 2020, from https://www.volkskrant.nl/nieuws-achtergrond/aivd-zat-ten-tijde-van-mh17-niet-in-kiev~ba73050a/

NOS. (2014, July 17). 298 doden bij Malaysia-crash. Retrieved March 6, 2020, from https://nos.nl/artikel/676034-298-doden-bij-malaysia-crash.html

NOS. (2014, July 18). Nederlandse delegatie in Kiev. Retrieved March 6, 2020, from https://nos.nl/artikel/676618-nederlandse-delegatie-in-kiev.html

NRC. (2014, June 20). Veiligheidsdienst AIVD verliest zicht op escalerend jihadisme. Retrieved March 10, 2020, from https://www.nrc.nl/nieuws/2014/06/20/veiligheidsdienst-aivd-verliest-zicht-op-escalerend-jihadisme-a1424214

Trouw. (2014, July 19). "Rebellen halen lichamen weg." Retrieved March 6, 2020, from https://www.trouw.nl/nieuws/rebellen-halen-lichamen-weg~b0569013/?utm_source=link&utm_medium=app&utm_campaign=shared%20content&utm_content=free

Trouw. (2014, July 23). Telefoons slachtoffers MH17 zijn niet preventief af te sluiten. Retrieved March 6, 2020, from https://www.trouw.nl/nieuws/telefoons-slachtoffers-mh17-zijn-niet-preventief-af-te-sluiten~b86ce83e/