



# Security Management in a Peace Observation Mission

Abraham Edel

2019 Laurea



Laurea University of Applied Sciences

**Security Management in a Peace Observa-  
tion Mission.**

Abraham Edel  
Security Management  
Bachelor's Thesis  
April, 2019

Abraham Edel

**Security Management in a Peace Observation Mission**

Year	20192019	Pages	37
------	----------	-------	----

---

The aim of this thesis is to provide an understanding of how the concept of security is looked upon at, and how security regulations are being implemented and organized in peace observation missions, within the framework of Civilian Crisis Management (CCM). This thesis has been carried out as a research project. The topic was chosen independently by the author, and not as an assignment by a beneficiary, due to the fact that the political pressure in missions can be very high. Any thesis conclusion could easily be interpreted as contradictory, or in favor of one of the party's interests.

The objective in this thesis is to see whether common security theories are used, to what extent, if there is space for improvement and in that case what kind. The knowledge base in the thesis is constructed on a combination of the author's own work experience of twenty years within security and civilian crisis management, and an extensive use of the most relevant literature and electronic publications within the field concerned.

The research method used, is the participating observation method. This method was chosen, due to the fact that the author currently works in a peace observation mission. The author intensively observed and personally experienced the phenomena and procedures concerned, on the spot, during a period of six months.

The main conclusion of this research project is that improvements could be made regarding the security regulations in the peace observation mission, within the framework of Civilian Crisis Management (CCM), which the author used for this research project.

Instead of implementing general mission wide security risk assessments and using general security regulations, it could increase the effectiveness of the mission if the mission instead would implement tailor made security regulations and security risk assessments. The security regulations and security risk assessments could for example be based on the current situation in a specific area, instead of focusing on the general security situation in the country. In this particular research case, the security principles of TEAR and ALARP were used, but not in the most effective way.

Since the political pressure in Civilian Crisis Management missions can be very high, a tendency that the security design is not focused on effectiveness, but rather on prevention of any type of liability, can sometimes be seen.

Keywords: Civilian Crisis Management, Security, ALARP, TEAR, Peace observation.

## Table of Contents

1	Introduction .....	6
1.1	The context of the research .....	7
1.2	The aim of the research .....	7
1.3	Research Questions .....	8
1.4	Possible outcomes of the research HYPOTHESIS .....	8
2	Theoretical Framework.....	8
2.1	The ALARP principle .....	8
2.2	The TEAR principle .....	10
2.3	Limitations in Risk Mitigation. ....	11
2.4	Security Design .....	12
2.4.1	Finding the balance between security and Risk. ....	12
2.4.2	Security as added value.....	13
2.4.3	The Best Security System Is that Which Employs the Most Efficient Combination of Equipment, Manpower and Procedures .....	14
2.4.4	Security = Cost + Inconvenience; Good Security = Less Cost + Less Inconvenience .....	14
3	Research Methodology.....	15
3.1	Participating observation method .....	15
3.1.1	Living in the context for an extended period of time .....	16
3.1.2	Learning and using local language and dialect .....	16
3.1.3	Using everyday conversation as an interview technique and research tool. ....	17
3.1.4	Informally observing during leisure activities (hanging out). ....	17
3.1.5	Recording observations in field notes .....	17
3.2	Research environment .....	19
4	Implementation - conducting research .....	20
4.1	Project organisation and cooperation .....	21
4.2	The different stages in the implementation .....	22
5	Findings .....	23
5.1	Who is in effective charge of the security measures during the monitoring components of the missions? .....	23
5.2	How do the security measures which are in place work? .....	26
5.3	How do the security measures influence the work of the monitors on the ground? .....	29
5.4	Does using of the ALARP principle enhance productivity? .....	30
6	Conclusions .....	30
6.1	Reliability and Validity .....	32
6.2	Further research subjects .....	33
	References.....	34

## List of Abbreviations

ABL	Administrative Boundary Line
ALARP	As low as reasonably possible
CCM	Civilian Crisis Management
CSDP	Common Security and Defence Policy
ENTRI	Europe's New Training Initiative
EU	European Union
EUEA	European Union External Action
EUMM Georgia	European Union Monitoring Mission in Georgia
HEAT	Hostile Environment Awareness Training
HO	Head Office
HoM	Head of Mission
ICRC	International Committee of the Red Cross
ISMI	International Security Management Institute
ISO	International Standard Organisation
JCCC	Joint Centre for Control and Co-ordination
NATO	North Atlantic Treaty Organisation
OSCE	Organisation for Security and Co-operation in Europe
PPE	Personal Protection Equipment
RNLA	Royal Netherlands Army
SMM Ukraine	Special Monitoring Mission in Ukraine
SOP	Standard Operation Procedures
SRA	Security Risk Assessment
TEAR	Transfer, Eliminate, Accept or Reduce
UAV	Unmanned Aerial Vehicle
UN	United Nations
UNSMIS	United Nations Supervision Mission in Syria

## 1 Introduction

This work consists of six chapters. In the first chapter, I will introduce the context and the aim of the research. In the second chapter I will present the theoretical framework. In the third chapter I will explain the basics of security design followed by the fourth part where I will present and describe the methodology of the research and explain how the research was conducted. In the next chapter I will present the implementation of the research methods. Finally, I will summarize the findings of my study, in the light of the theoretical framework, and propose ways how the findings could be used to improve the current.

Civilian Crisis Management is defined by the European Union in the following way; *“Civilian crisis management describes a policy which involves the deployment of civilian assets in response to an ongoing crisis, to tackle the consequences of a crisis or to address the causes of instability”* (Tardy, 2016). The interest in this topic has grown bigger as a result of increasing work in international missions, especially since not much research has been done in this area before. One example of the increasing interest is the formation of improving the effectiveness of capabilities in EU conflict prevention (IECEU). This is an EU funded organisation which has as goal, according to the website of the IECEU (2018), *“to analyse the current situation of ongoing and past EU CSDP missions, learning from lessons from these EU CSDP missions and providing new solutions, approaches and recommendations for the EU to guarantee long-term stability through conflict prevention and peacebuilding.”* Although there are many publications on the topic of civilian crisis management, many from the IECEU, none of them focus on a tactical or operational level, with IECEU publications focusing on the strategic level.

The organisational infrastructure and role of civilian crisis management has grown enormously in recent years; according to the website of the European Union External Action (EUEA, 2018) the European Union alone has had 17 civilian crisis management missions in the last decade. Peace keeping has changed a lot in this time, as have the needs of civilian interventions, particularly in contexts where they combine with military missions. It is important to note that these are unarmed missions, and that an armed backup may not always be available. This means that, in thinking about Civilian Crisis Management, a comprehensive security approach is often favoured. Although there is not a widely agreed upon definition of comprehensive security, the Austrian Institute of International Affairs writes in their paper ‘Concepts of Comprehensive Security’ that the idea behind ‘solving’ a conflict has changed over the years, but especially during the so-called war on terror. The author of the paper (Raab, 2011) states that *‘Comprehensive security [implies that] Security has to be understood not only as mili-*

*tary and state security, but as well under the aspects of other socio economic factors and the integrated, subjective feeling of security or insecurity of individuals in a certain society*'. With this developing understanding of security beyond the purely militaristic approach, civilian peacekeeping mission have gained a larger role than they had before.

A civilian peace observation mission has the purpose of checking whether a cease fire or peace agreement is being observed. This could be for a cease fire agreement (such as the OSCE Special Monitoring Mission in Ukraine) a peace agreement (European Union Monitoring Mission in Georgia) or any other similar type of agreement between two parties. The task of these types of missions is not to intervene in the conflict, but purely to observe and report to their respective organisations. This could also be bilateral, as in the Joint Centre for Control and Co-ordination, which is a bilateral initiative between the Russian Federation and the Ukraine, or even multilateral, like the OSCE Treaty on Open Skies (OSCE, 2018) which operates between the relevant state parties and gives the state parties the possibility to observe each other's armies and military installations.

Because of the complex and often sensitive specific contexts in which a peace monitoring mission must function, it is often difficult to conduct independent surveys on the role and effectiveness of the security in these missions.

### 1.1 The context of the research

The focus of the thesis will be on unarmed civilian monitoring mission. The reports these missions produce are the only tangible product a mission of that type and style has. The nature of a peace observation mission is quite unique. It is already difficult to compare a commercial organisation with a non-profit organisation, and even more so to compare a commercial organisation with a peace keeping organisation. When we look at the websites of the UN (2018), EU (2018) and the OSCE (2018) then we can see prominently the information about the observations on the ground by the monitors. This information is used to inform either a higher organisation (for instance the security council of the UN or the OSCE permanent council), but it can also been used to inform the member states.

### 1.2 The aim of the research

The aim of this research is to increase understanding of what security measures are in place in peace observing missions, how are they organised and how security measures influence the primary function of these missions. The security measures discussed will also be compared with the measures which are taken with the ALARP (as low as reasonably possible) principle and the TEAR (Transfer, Eliminate, Acceptance and/or Reduce) principle. Because of this, the aim of the research is; *'to assess the function and impact of security measures on the field work in a peace observation mission'*.

### 1.3 Research Questions

The research questions are as follows;

- Who is in effective charge of the security measures during the monitoring components of the missions?
- How do the security measures which are in place work?
- How do security measures influence the work of the monitors on the ground?
- Would it be more productive to work according to the ALARP principle?

The purpose of this research is to show whether appropriate security risk analyses and the ALARP principle are active in peace observing missions. The focus is on the monitor on the ground, whose actual observations will form the bulk of the reports.

### 1.4 Possible outcomes of the research HYPOTHESIS

The research aims and research questions can be summarised as follows:

*To assess the effectiveness and the impact of security measures on the field work in a peace observation mission'*

There are two parts to the research aim. One is how the security measures are implemented and how they are used. The second part is about how the security measure affects the core work, the actual monitoring.

In both parts of the thesis there are three possibilities: that the measures work, do not work, or work to some extent; that the measures influence the observation, do not influence it, or influence it to some extent. I expect that the outcome will be that the security measures are working, but that the measures influence the observation possibilities of the staff.

## 2 Theoretical Framework

In this thesis, several principles will be used as a framework for the research: the ALARP principle, and the TEAR principle. In what follows both principles will be introduced and discussed.

### 2.1 The ALARP principle

The origin of ALARP does not come from a security or a commercial background, but from health and safety. The principle was used to define much action an employer had to take to protect his employees.

Jones-Leem M and Aven, T, notes that “the first formal definition of ALARP was provided in the English courts. Specifically, in the Court of Appeal in *Edwards vs. National Coal Board* [1949] the judge’s ruling was to the effect that: ‘Reasonably practicable’ is a narrower term than ‘physically possible’ and seems to me to imply that a computation must be made by the owner, in which the quantum of risk is placed on one scale and the sacrifice involved in the measures necessary for averting the risk (whether in money, time or trouble) is placed on the other; and that if it be shown that there is a gross disproportion between them—the risk being insignificant in relation to the sacrifice—the Defendants discharge the onus on them.” (2011, s.4)

In addition, the issue of reasonable practicability was considered by the House of Lords in *Marshall vs. Gotham & Co Ltd* [1954] AC360, the head note of which states: The test of what is (reasonably practicable) is not simply what is practicable as a matter of engineering, but depends on the consideration, in the light of the whole circumstances at the time of the accident, whether the time, trouble and expense of the precautions suggested are or are not disproportionate to the risk involved, and also an assessment of the degree of security which The measures suggested may be expected to afford.

The meaning of ‘gross disproportion’ is especially important to a proper understanding of ALARP. In *Edwards vs. National Coal Board* above, we can see what the court meant by use of the phrase (that the risk is insignificant in relation to the sacrifice). Although here the reasoning comes from a health and safety background and the court case was about the responsibility of the employer, this principle has developed further to play an important role in commercial security theory.

The motivation for ALARP is to find a balance between cost and security. The ALARP principle is the most common principle used within security for this purpose. It is premised on the idea that every risk can be mitigated to some extent. However, this comes with certain costs to facilitate these mitigation measures. For instance, it is possible to transport an egg with zero chance that it will break. But if we transport the egg according to the ALARP principle, and with the price of an egg somewhere around 8 cents, then the costs of keeping the egg intact become unreasonable.

This does not only affect profitability, but also usability. For instance it is possible to have a safe internal network, with almost zero chance of any information being stolen. If the network is not connected to the internet and every user has a three way access authentication, than one can reasonably assume that the network is safe. However, a network without access to the internet is not very useful, and to use a three-way authentication is not very user friendly. If one than adds the cost to the usability, it comes clear that maximum risk mitigation is, once again, unfeasible.

The ALARP principle applies to a various groups within a company. It also applies to the legal unit. For instance, how far will one go in taking insurance? The Royal Netherlands Army for instance does not have insurance on their vehicles (Ministerie van Defensie, 1999). Although insurance would mitigate risks, the costs are prohibitive. It is more effective for the RNLA to repair vehicles in the case of accident and pay compensation itself where necessary.

In the end, it a decision must be made as to where to strike the balance, but that decision should always involve a similar cost/benefit analysis, whether these are financial, practical or anything else.

## 2.2 The TEAR principle

A key part of effective security management is to be pro-active in identifying the risk. By being pro-active, mitigating measures can be in place before something happens, thereby mitigating any negative effects. However, the question of what mitigating measures to take is a complex one. There are many available options for risk mitigation, but they can all be assessed using a second principle: TEAR. This TEAR stands for Transfer, Eliminate, Acceptance and/or Reduce the risk. Although there are more variations from this principle the author will use this variation as described in the ISMI manual (2014a). These options should be decided upon, with the needs of the operation in mind as well as the relative riskiness of its various elements.

Transfer of risk means a transfer of the responsibility of the risk to a different target or organisation. The idea behind this is not that somebody else becomes the target of the risk, but that the impact of the incident is being carried by somebody or something else. For instance, if we look at the European Union Police Mission in Afghanistan, the unarmed civilians are protected by commercial close protection teams. These companies are hired, in part, to take over the responsibility of the risk. If we look at the European Union Monitoring Mission in Georgia, the risk is transferred to the local authorities, who take over the responsibilities of the protection of the monitors during patrols if needed. However, what is most common is the transfer of the risk to an insurance company. In this case the insurance company takes over the impact of the risk.

A security risk can normally not be eliminated just by security measures. In fact, one can only eliminate risks associated with an action by not doing it. Almost all peace observation missions are in countries where the roads are bad and traffic rules are not strictly enforced. Obviously this increases the risk of having a road traffic accident, but the only way to eliminate this risk is to stop participating in traffic. This is obviously nor a desired outcome, because it presents a huge obstacle to the effectiveness of the operation. However, sometimes this is the only option: for example in 2016 a forward patrol base was evacuated because of nearby shelling (OSCE, 2016). The fighting became so intensive that the risk of having staff injured or

even killed became too high. This is perhaps a measure which is not taken that often by commercial companies, but for instance it has happened in the Netherlands where a nuclear power plant was being decommissioned, due to the fact that the already existing mitigation measures were not considered adequate. Another example is the operation of the International Committee of the Red Cross (ICRC) in Yemen (Wintour, 2014). When the hospitals were being bombed and with no option for negotiation, the ICRC had no other option than to withdraw their international staff.

Sometimes risks are just too rare or the impacts too insignificant for it to be worth taking any measures against, and so it must be accepted. For instance, the risk of staff stealing minor office equipment, like stationary, is too insignificant to be worth managing. Similarly, some risks are too remote to be worth mitigating. If we again look more specific at peace observation missions, for instance the OSCE SMM mission, we can see that one of the risk mitigation measures is that the monitors wear flak jackets and helmets, and they drive around in armoured cars. These measures are aimed to protect the monitors against handheld fire arms and shrapnel from a mortar attack. In the judgement of the security cell of the mission, this is the biggest risk. Although there is also the risk that a monitor can get hit by a projectile which is fired by a tank, the security cell judged that this risk is too remote to manage, especially given the lack of available resources to mitigate this risk.

By far the most common measure found in TEAR is the reduction of risk. An organisation will always try to reduce risk. For instance, if we look at the European Union Monitoring Mission in Georgia, the patrols close to the contact line have an ambulance following them. Due to the lack of medical care the mission believes that this reduces the risk of monitors getting permanently hurt in the event of an accident. Similarly, monitors are obliged to wear personal protection on their torso and on their head; an example of reducing the risk of getting fatally wounded by gunshots or shrapnel. It is important to note that the elements of TEAR are not necessarily exclusive; such personal protective gear might constitute a measure to *reduce* one risk, while also constituting an *acceptance* of another (a risk for which a vest or helmet would be ineffective protection).

### 2.3 Limitations in Risk Mitigation.

Even with the best intentions and the best ideas, there are often barriers to implementing security regulations. This also work the other way around: existing security regulations may interfere with what would otherwise be considered ideal plans. Blyth (2008) identifies three such barriers: Customer access and Expectations, Compliance with Regulations and Budgetary Constraints.

The first one, customer access and expectations, varies greatly depending on the culture and nature of a company. However a customer always has a certain expectation of how his expe-

rience will be or how the product is what he is going to buy. So as a business person you do not want the security measures interrupting the experience. An example for this is Disneyland Paris. When one leaves the train station, Disney is already trying to get their customers in a certain atmosphere. However this is interrupted by the presence of French soldiers who are there in an anti-terrorist task. For a lot of people, this is not what you expect when you go to a theme park. Football supporters are another example. The author has seen from his professional experience as a police officer that to prevent riots and unwanted behaviour in football stadiums, the security checks are of a very high level. Often you have to be a member of the football club, and have a certain security clearance to be allowed to go to away games. This is a large obstacle for supporters to buy a ticket. The business goals determine that the focus should always be to get as many (satisfied) customers as they can get.

Secondly, not all security measures are live options for a company. Often countries have their own sets of legislation for security and mitigation measures. The ALARP principle is one example, founded as it was in the courts. As such, one must always be aware of local legal requirements. This also works the other way around. You might think you need armed guards, but if this is not allowed by law this measure will be impossible.

Finally, there are budget constraints. Of course one can wish for all kind of measures and regulations, but when there is no money to implement them, it is simply not possible. This is an issue in most companies, as security is not a (direct) income stream. This is one reason the role of the security manager is so vital, as they must convince the board to make the finances available for necessary security measures.

## 2.4 Security Design

Security design is an incredibly broad topic, involving everything from building plans and parking rules to training security guards. To keep things simple, I will focus here on the core function of the design of security plans. Other factors, like political influence, geopolitical context and logistic measures will be set aside for reasons of scope. There are several ways to approach the issue of security plan design, but we will take the 18 security planning principles put forward by ISMI (2014b) as a starting point. We will focus on four, which are all relevant to the ALARP principle, while the other 13 principles concern actual physical security design.

### 2.4.1 Finding the balance between security and Risk.

This principle describes the core of security management. Before starting any security design, the security cell should make a proper risk analysis. According to Broder (2006), a risk analysis follows a simple formula;  $\text{Asset} + \text{Threat} + \text{Vulnerability} = \text{Risk}$ . An asset is something which the organisation wants to be protected. A threat is what the organisation is protecting the asset against. The vulnerability is the weakness which could threaten the safety of the asset.

All these three things combined is a risk. The measure the company takes against this risk has to be in balance with the risk. This is where the TEAR principle comes in.

As an example, the principle asset of EUMM Georgia is the monitors, who drive around, mostly in unarmoured vehicles. However, there are a few minefields. This is a **threat**. The fact that most of the vehicles are unarmoured creates vulnerability if the vehicle with the monitors would hit an anti-tank mine. These three combined gives the risk of an unarmoured vehicle, with monitors inside, hitting an antitank mine. Now the security advisor has to come up with a security measure which to protect against the threat, which is in balance with the actual risk. If the security manager understands that the monitors almost never have to go to the mined area, it is not in balance with the actual risk to force all the monitors to drive around in armoured cars. In this case it was better to simply forbid the monitors to drive in the areas where there could be anti-tank mines. This would cost nothing and have almost no impact on the actual operations.

#### 2.4.2 Security as added value.

Kovacich and Halibozek (2003) say that one of the issues with creating a security budget is as following. Security is usually seen as a cost centre and not a revenue-producing entity; therefore, it is in competition with other (internal) organizations for budget. How that budget is obtained varies and is often dependent upon the demonstrated added value of the assets protection or security program to the organization. Because of this, it is of the utmost importance that the security manager shows that security measures make money, instead of just costing money. If we look at retail for instance, we can see that shoplifting is a huge cost. According to a survey done by Hollinger (2017) the retail sector in the United States lost around 50 billion US dollars to shoplifting in the year 2016. The key for the security manager is then to explain that the security measure does not just cost money, but in fact makes money by preventing loss to theft. When the costs of the theft decrease, the profit increases. The problem with making this case is that this is not easily visible or even easy to predict, whereas for instance profit driven by sales or investments in development are far easier to demonstrate.

The budget of the OSCE SMM is according to the OSCE website currently 137million USD per year. The SMM has operated since 2014 and so far there has been one fatal casualty. The Russian Federation has proposed to have a UN peacekeeping mission in the Eastern part of the Ukraine with the main function of protecting the OSCE SMM monitors. So far, this proposal has not found any supporters; due to the fact that the security measures are working and 'only' one monitor has died (the lack of support may also be due to various geopolitical reasons). However, if the support increased, a UN military mission along these lines could be deployed. According to the Ukraine envoy to the UN, Volodymyr Yelchenko, this would cost a billion USD per year (UNIAN, 2017). I try to show here that because of the security measures in place in

the OSCE SMM, there is no need to replace that mission with a larger peacekeeping mission. Therefore the international community saves a lot of money.

#### 2.4.3 The Best Security System Is that Which Employs the Most Efficient Combination of Equipment, Manpower and Procedures

The third principle which ISMI (2014b) puts forward concerns not just the functioning of security measures, but also the efficiency of the combined assets which are needed to implement them. For instance, ISMI discuss the protection of industrial buildings in the UK. These are commonly not very well protected in terms of physical security. This is partly attributable to the security culture in the UK, which historically relies more on system security. As such, the system security is often great, but is frequently not enough alone. If we look again at peace observation missions we can take UNSMIS (United Nations Super Vision Mission Syria) as an example. The UNSMIS, which was an unarmed peace observation mission, deployed for less than six months in Syria; the mission had to be cancelled due to increased security risks. UNSMIS involved a huge combination of security measures for the purpose of protecting the monitors on the ground. First, personnel: They were all professionals in their field and most of the monitors had previous experience in missions or in hazardous areas. These monitors were wearing personal protection equipment and were trained in negotiating with the fighting parties. Then there was the backup from the forces of the United States, which worked like a big stick. Although this mission had to be cancelled because the risks became too high, they could perform for quite a while through these combinations of measures (Gowan, 2012). But here it is important to understand what the most efficient combination is. For instance, the OSCE SMM in Ukraine is right now the most efficient option. A military mission is out of the question due to political hostility, and would cost a lot of money and would need a huge amount of manpower; and the no-mission option is not acceptable for the international community.

#### 2.4.4 Security = Cost + Inconvenience; Good Security = Less Cost + Less Inconvenience

In 1987, Col. Paul Roos, who worked as a security advisor for Shell in Africa, come up with this principle. ISMI (2014b) discusses it in the following way:

*‘Security systems and operations should be designed to be cost-effective, delivering value for money and simultaneously causing as little inconvenience to both the corporate operations and individual employees. From an employee’s point of view, well trained and managed security personnel will cause less inconvenience and thus make security more acceptable’.*

Good examples of this are security updates which computers do automatically as a part of the software purchase; users can choose when the updates are installed, and the updates ensure that the software is always functioning properly. Therefore this is perfectly in line with the Roos principle.

### 3 Research Methodology

Due to the type of objective in this research and the fact that the author is currently working in a peace observation mission, “participating observation” has been chosen as the most suitable and effective empirical method to collect data for this project.

One of my research questions is to identify the impact of the security measures on the main work of peace observation missions. Because there are no easy ways to measure the productivity of these missions, a participatory methodology will allow the impact of security measures to be described. It is important to note that this is a subjective approach. The findings come from people, who will give their opinion to the researcher, who will transform this into information. The author will then critically assess this information, and attempt to answer the research questions based on that assessment. The qualitative and subjective nature of the research means that it is vital to keep the balance into what is valid and what is not for the methodology. It is also important to put the findings in the right context. Therefore, it is vital that the author be part of the test group. DeWalt and DeWalt (2002) (described below) have written on how to effectively use this kind of methodology in research.

#### 3.1 Participating observation method

The participating observation method has its roots in ethnographic research. It is a qualitative research method which is used mostly in sociological and anthropological studies. It is “a method of research in anthropology which involves extended immersion in a culture and participation in its day-to-day activities” (Calhoun, 2002).

According to DeWalt and DeWalt (2002, 92), “*the goal for design of research using participant observation as a method is to develop a holistic understanding of the phenomena under study that is as objective and accurate as possible given the limitations of the method*”. Participant observation involves a combination of interviewing, document analysis, questionnaires and interviews, from which theories can be built to generate or test hypotheses.

According to DeWalt and DeWalt (2010) the following seven key elements are normally involved in the participating observation method;

- Living in the context for an extended period of time
- Learning and using local language and dialect
- Actively participating in a wide range of daily, routine, and extraordinary activities with people who are full participants in that context
- Using everyday conversation as an interview technique

- Informally observing during leisure activities (hanging out)
- Recording observations in field notes (usually organized chronologically)

### 3.1.1 Living in the context for an extended period of time

There are numerous examples of researchers who lived together with their research subjects. DeWalt and DeWalt (2010) give examples of research about poachers (Brymer), about the trade in narcotics (Adler) and street children (Hecht). They all agree that living with their subjects was a vitally important part of understanding their subjects. They also quote one particular researcher, Desjarlais, who writes the following about his participating observation experience in becoming a Yolmo Shaman; *'Through time, experiencing the body in this manner (including the residual, intermingling effect it had on how I stepped through a village, climbed a hill, or approached others) influenced my understanding of Yolmo experiences; it hinted at new styles of behaviour, ways of being and moving through space that I did not previously have access to. By using the body in different ways, I stumbled on (but never fully assimilated) practices distinct from my own. Touching head to heart merged thinking and feeling (two acts unsegregated in Yolmo society); a sense of the body as a vessel dynamically compact led me to see Yolmo forms as vital plenums of organ and icon; and my loose assemblage of bent knees and jointed bones contributed to the springboard technology that gradually brought some force and ease to my shamanic shaking'*

In the case of this research, it is important to be a participant in the whole process. This has made it possible to gain special insight into the subject, especially considering subjective experiences such as feelings of safety and similar impacts of safety regulations on the monitors.

### 3.1.2 Learning and using local language and dialect

Robbins, a motivational speaker said the following about communication; *"To effectively communicate, we must realize that we are all different in the way we perceive the world and use this understanding as a guide to our communication with others"*. Although in the research, the participants all speak English, as this is the main language used in this peace observation mission, the diversity in cultural background is immense. If we take the OSCE as an example, there are 57 participating states, with various ethnic groups within these countries, with different religions and different professional backgrounds. The fact that all participants speak the same language, therefore, doesn't necessarily mean that there will be flawless communication. The advantage the author had in this respect is that he has extensive experience in the field of peace keeping and especially in peace observation missions. Thus, he has shared experiences to draw on with the participants in the research in order to facilitate communication.

### 3.1.3 Using everyday conversation as an interview technique and research tool.

Interviewing people can be done in various ways. From long extensive interviews to surveys, closed questions and open questions, the options are numerous. However, in the participating observation method, the central idea of the participant observation method is that the researcher should be a part of the group being studied. The risk of formal interviews is that this might threaten that dynamic. Especially if the researchers only have one or two interviews with the actual subject, it might be difficult to build up sufficient trust between the researcher and the subject. Whyte (1984, 69) writes the following *“Go easy on that “who,” “what,” “why,” “when,” “where” stuff, Bill. You ask those questions, and people will clam up on you. If people accept you, you can just hang around, and you’ll learn the answer in the long run without ever having to ask the questions”*.

The author has experienced this in person during his work in various missions. Especially after having worked together and experienced difficult and challenging situations, people are comfortable speaking about those experiences. Information gained in this way, and especially during after action reviews, was very helpful in this research.

### 3.1.4 Informally observing during leisure activities (hanging out).

In participating observation research there is no single way of conducting research, a lot is depends on the subject and the test group. When we look at the examples given in 4.1 we see that Desjarlais had to completely immerse himself in his test group, otherwise he would not have become a shaman and thus not have reached his goal. However, Adler, in his research in the trade of narcotics had to keep a certain distance as the trade was criminal and involved a lot of violence. Because of similar limitations on certain test groups give, it is important to observe the test group also when they are not performing the actions which are the central focus of the research. This helps in gaining trust and establishes respect from the test group.

In the case of this thesis, this was less relevant. Due to the fact that the test group lives together in one location and rarely has the opportunity to go elsewhere unless working, respect is gained by sharing in that work, and all leisure time is spent together by default. In fact, there is no clear demarcation between the working time and leisure time.

### 3.1.5 Recording observations in field notes

Due to the nature and length of the research, the amount of data the researcher gained is enormous. Some data is useful, some is not, and some might become useful later. In addition, due to the length of the research and the fact that the researcher is present throughout, it might be difficult to see small changes or notice slow progress. This is why it is important to keep field notes that can allow such progression to be tracked after the fact. DeWalt and DeWalt (2010) identify various methods of making field notes. For instance ‘jot’ notes which

are keywords written in the moment in, for instance, a small notebook. Bernard (2006) writes about methodological notes. These are notes written with an emphasis on the methodology. So, for instance, about how the methodology was implemented or what kind of issues were encountered and how these were solved. Several researchers (Sanjek, Bernard, Malinowski) write about the use of journals and diaries. The advantage of using these is that one has a chronological order of one's experiences. However, DeWalt and DeWalt (2010) claim that this is often not practical during fieldwork. A log is more practical, as it creates an overview of all the notes and it is also chronological. One method, rarely used now, is the use of meta-notes. These notes were used to analyse other field notes. This method is not much in use anymore, as computers make it a lot easier to store and carry around all notes. Finally, DeWalt and DeWalt (2010) write about headnotes. These are mental notes kept in one's own head. Obviously this is not the most reliable method, but will be used by any researcher. The big advantage of these notes is that you cannot lose them, as long as they are not forgotten. DeWalt and DeWalt (2010) write about the case of a researcher called Srinivas, who lost all his notes which he had gathered during 18 years of research. This meant that he had to write his book completely based on memory. One must keep in mind however that head notes are not always reliable, based as they are entirely on memory.

In a normal working day, the author would start in the morning by participating in the morning briefing. During this briefing one hears what the current situation is in the area of responsibility, and will receive the security briefing. The next phase is to have the next briefing, which is specific to the current tasks of the patrol. Observations are very important during these two phases in order to gauge the immediate impact of the security assessments on the monitors. Due to the social cohesion in the team, the monitors are eager to express their views on these issues. Lots of useful observations were made at these times. Next is the patrol briefing, where a plan is made to reach the mission's goals. In this phase the limitations of the security regulations become truly visible, so this increases the rate of change in the discussion and requires a lot of the monitors to adjust their plans; making sure that they can make the most of patrolling, while obeying the security regulations. During the actual patrolling, the author was often with one or sometimes two persons in the patrol vehicle. These were the moments to seek the in-depth views of the monitors regarding the security regulations.

It is also important to take the nature of the source in consideration. A young professional who just started their career might have a very different view than, for instance, somebody who is already retired. Their professional background should also be taken in consideration. In general, people with a military background have a very different approach to issues they might face in work than somebody with, for instance, an academic background. Everybody looks at things from their own perspective, informed by, among other things, their background and experience.

### 3.2 Research environment

The author works currently in a peace observation mission. This mission is divided in several core teams which operate throughout the country. The team in which the author works has their area of responsibility at the front line. As such, security threats and regulations have an extremely high impact on their work.

This team consists of 22 monitors. These monitors have the task of peace observation, making assessments of the situation on the ground and writing reports about their observations. These reports are sent to the mission headquarters. These reports are analysed and sent on to the organisational Head Quarters and member states, and are then used in peace negotiations.

The monitors have backgrounds in either law enforcement, the armed forces or as civilian experts. The requirement to be part of a mission like this is to have at least eight year of working experience and/or a master's degree in a relevant subject and/or a rank higher than captain or equivalent. Since the author is part of this team, he will talk and listen to the monitors and team leaders. Also, he will undergo the personal and professional impacts of the various security measures. Because of the position of the author, he will be able to see and hear the reactions of the monitors, but also of the local population and NGOs who are working in the area. Finally, the author will also experience how the fighting parties are using the security regulations to their advantage.

Due to regulations and security concerns from the organisation the author works for, it is not possible to reveal the name of the organisation or any details of the mission. This makes it also difficult to fully explain how the organisation is constituted, however the author will use his experience of the various missions he has worked in to build a general picture for the reader of what such missions usually look like.

Most of the missions operate in warzones, post-conflict areas or at least very politically unstable areas in the world. Some of the peace observations missions are in relatively peaceful areas, like the UN mission in Cyprus or the EU mission in Georgia. In these countries there is no active war, but instead a standoff between two sides, a so-called frozen conflict. Some missions are in full combat zones, like the OSCE missions in Ukraine or in Nagorno-Karabakh. In both areas, there is still fighting every day. In the countries in which these missions take place there is still a functioning government. In certain countries, the security situation has deteriorated so heavily that the mission is completely evacuated or has never been deployed, like the EU mission in Libya.

Although all missions are different, the organisational structure is often similar. Most follow the structure which Hardy and Runnels (2014) advice and which is also written in the ISO standard 31000:2018. The organisational structure is often such that there is a head of mis-

sion who bears overall responsibility for the mission. I will discuss the organisational structure of missions more in the findings.

#### 4 Implementation - conducting research

DeWalt and the DeWalt (2010) suggest four questions which the researchers have to ask themselves, before starting their research.

First, is the topic important enough to research? For the various reasons given above (efficiency, cost reduction, focussing on the result) the author believes that this research will be a valuable contribution to making positive changes to the effectiveness of peace observation missions.

Secondly, will answering this question produce new knowledge? There is quite a bit of research on peacekeeping, about the role of peacekeeping missions in conflict areas (and especially on the role of gender diversity in such missions), however the author could not find any security management research with a focus on peace observation missions. Hence, answering the present research questions will absolutely produce new knowledge.

Thirdly, is this the right research site to conduct this research? The research site, and the locations of the test group, is a field office operated by the peace observation mission. The persons in the test group are all working in this mission and are all professional in their work. This test group consists of the people who create the mission reports, and are the ones most directly affected by the security measures, but due to proximity to the front line, also the among those most affected by the conflict. During the research the group had 23 members, between 31 and 62 years of age. They come from 15 different nationalities and have backgrounds in law enforcement, the armed forces, international relations and human rights. In the test group there were 19 men and 4 women.

The fourth question is whether the theoretical approach/conceptual framework is valid for this research? The framework is based on the ISO 31000 and the ALARP standard. The ISO standard is used worldwide and is seen as one of the two main standards within security management. As Gjerdrum and Peter (2010, 12) describe it; *“A real strength of this new ISO 31000 risk management approach is the identification of risk owners and the necessary wide-spread education about risk—both within and without your organization. It increases accountability and strengthens communication. The link to business objectives (at all levels) strengthens both the relevance and the importance of risk management. Ultimately, the ISO 31000 standard provides a vehicle to make risk management central to the success of an organization, and an intimate part of key processes such as planning, management and governance”*.

The ALARP principle is in general the core of any security management structure. Aven and Abrahamsen (2006, 346) write the following about the ALARP principle; “*The ALARP principle gives strong weights to the cautionary principle: The ALARP principle expresses that the risk should be reduced to a level that is as low as reasonably practicable. Furthermore, a risk reducing measure should be implemented provided it cannot be demonstrated that the costs are grossly disproportionate to the possible benefits obtained*”.

This leaves us with the question whether this is the right method to answer the research questions. As mentioned above, it is very difficult to assess the actual worth of a report when one does not understand the multitude of challenges the monitors face while operating in the field and when writing the reports. In the example given earlier, about the conflict in Georgia, the US senate did not know what the actual situation was on the ground. They could not assess the actual situation, as only the monitor on the ground can do this. The same applies to the impact of the security measures on the work. Therefore, the author believes that the participating observation method is the right method and perhaps the only method to answer the questions.

Also one has to question whether the project is achievable. With the experience the author already has, combined with the knowledge he gained during his studies and the preparation of the research, the author believes that the project as described is feasible.

#### 4.1 Project organisation and cooperation

Due to the immense political pressure on peace observation missions, the organisations operate very carefully to avoid causing political problems. Because of this, the author was not permitted to carry out the research openly. Therefore, there was no cooperation from the organisation itself, which caused challenges. Because the author works in the organisation, almost all security documents were available for the author, however the author could not use them in the research. Also many useful examples could not be used because of security concerns regarding the details of specific missions. Lastly, the author had to ensure that all field notes were carefully maintained and anonymized.

However there was cooperation on an operational and personal level with the colleagues throughout the research project. Because security measures are a day-to-day activity for monitors in every mission, sometimes greatly impacting their work, they are a frequent topic of discussion. The author’s colleagues were aware that the research was being done, and colleagues were told what the research was about. They gave their consent, as long as they could not be identified in the document.

#### 4.2 The different stages in the implementation

The author used the field guide of DeWalt and DeWalt (2010) to follow common procedure in participating observation research, which starts with 'entering the field'. This process is not just getting somewhere, but also getting used to where you are. In the case of the author, this is getting used to a highly hostile area and living in close quarters with the test group. Although the author had previous experience in civilian crisis management and in peace observation mission, the time to get used to the environment was very much needed. This was not only due to the hostile environment, but also to get used to live in such a different environment. It took the author a while to get settled in the area and to get to a certain experience baseline. Only when that process was done, the author could continue to the next phase.

After this (or even during), one must earn the trust of the test group by showing willingness and professionalism. In this phase it is also important to learn who is who in the group, and what role and function they all fulfil. Especially in a diverse group as this, it is also vital for the researcher to understand the differing backgrounds of every individual. In the current case, the author also had to understand the chains of command and organisational structure: How the mission functions, and who makes the decisions? This is what DeWalt and DeWalt (2010) call the 'first contact'. As described earlier, the test group is very versatile and very experienced. Due to the background of the author, having served as a professional soldier and as a police officer, it was relatively easy to connect to other people with that background, due to the same professional view on things. What was more difficult is to earn the trust of people with different cultural backgrounds. In certain cultures it's very unusual to comment on things your senior management decides.

According to the DeWalt & DeWalt (2010) after these two phases comes the 'establishing report' phase. After having fully understood where the researcher is, who the researcher is with, and what the working and living routine looks like, the research can start. This is a continuous process for a certain time in which the researcher observes talks, investigates and experiences what is going on, and begins to understand how the research questions are being answered.

In general this meant that while working with the test group, first of all the author needed to experience the work as such. One cannot do this for only a week or two, one really needs to delve into the environment and experience how it is, to work under the same pressure and to be in the same routines as the test group. So this is what the author did. The author worked with the test group as a regular member of the team for more than a month, before he started the research. This was easier than the author had expected. The author assumed that this was due to the fact that he worked as a full member of the team. The research was not the

core reason to why the author was present at the test site. The research project was conducted in addition to the author's regular work as a monitor.

During patrols the author verbally communicated with his patrol members and talked to them in a normal way, as co-workers do. It is challenging to make sure that the same questions are being repeated in the same order, to get the same pattern of answers. However, the author paid attention to this challenge throughout the research project and aimed at having a structured pattern of questions. In this type of work, as there is also a lot of waiting, there is space for extensive discussions on the general situation and the security situation. The topic is relevant for everybody in the mission, but especially for the people in the field. These circumstances made the information, which was needed for the research project, accessible.

For more than half a year, the author worked and lived together with the test group. After this time, the author assessed that there was enough information to answer the research questions. The phase is what DeWalt and DeWalt (2010) call the 'breakthrough'. This is the moment when, according to the earlier mentioned authors, all the gathered notes and information fall into place and the researcher can start to seriously assess how the research questions might be answered.

DeWalt and DeWalt (2010) describe two more phases, although these are integrated throughout the whole research. They are called 'Talk the Talk/Walk the Walk'; a matter of showing continuing willingness to work and participate in the group's activities, communicate effectively, and generally gaining the trust of the test group. Due to the position the author had as a co-worker, and not as visiting researcher, this happened in a natural manner.

## 5 Findings

After working for more than six months with the test group and following all stages of the participating observation method, there was more than enough material gathered to provide a fruitful analysis. First one needs to analyse the finding through the research questions.

### 5.1 Who is in effective charge of the security measures during the monitoring components of the missions?

Civilian Crisis Management (CCM) is different from a peace keeping mission in that there is no military style hierarchical structure. Although there is a certain hierarchy, it is different in that the average monitor has either a master's degree or vast experience within law enforcement or military affairs. The monitors are sent to the mission because of this experience. Therefore, it is expected that every mission member is capable of making his or her own decision and acting on them, but within a certain framework set by the mission management.

The security chain within CCM is organised separately from the normal chain of command. As we can see in figure 1 below, the chain starts within the Head Quarters (HQ) from the Head of Mission (HoM) to the operations department. The operations department is steering the teams in the field, which are divided into patrol hubs. These patrol hubs send out patrols with a patrol leader in charge. Finally, every monitor has their own responsibilities within the framework the mission management has set.

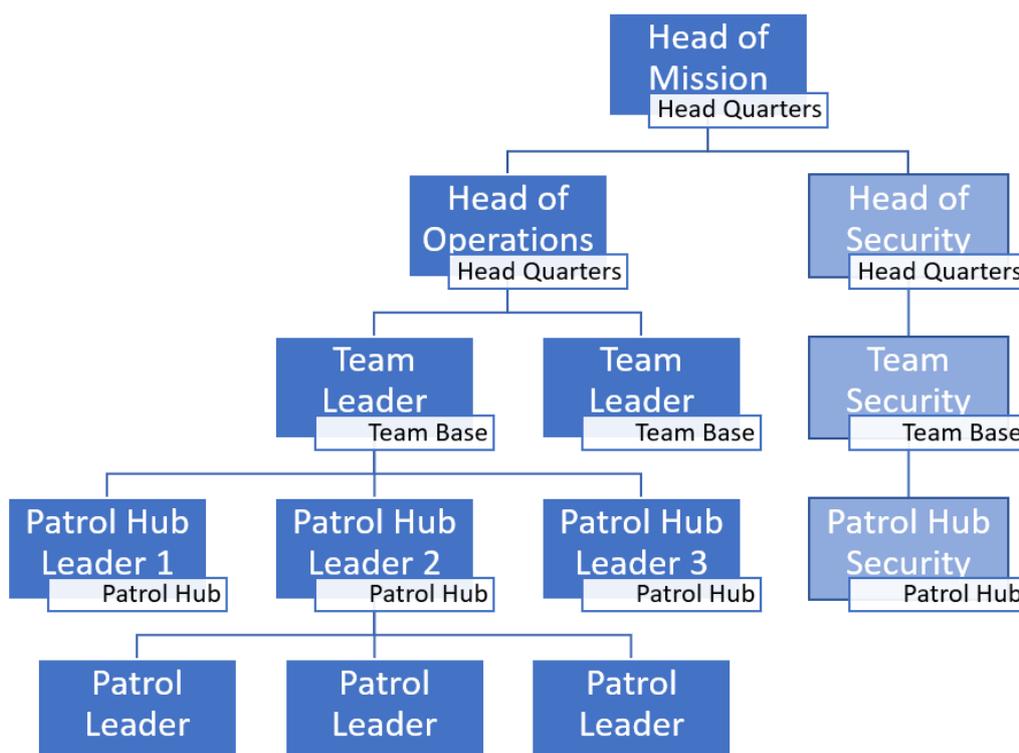


Figure 1: CCM Command Structure (2019)

What we can see here is one of the elements of TEAR in play. Reducing risk is not just a matter of mitigation against the threat, but also anything which might interfere with that mitigation. Due to a double chain of command and a network of overlapping responsibilities, the risk of making a mistake in decision-making or execution is brought to a minimum.

The organogram also shows that the security is not in the same chain of command as the patrols are. The head of security does not report to the head of operations, but directly to the HoM. It is also important to note that a substantial number of security officers are not seconded but contracted directly by the mission. Monitors and almost all other personnel are seconded from the participating state organisations by the organisation which organises the mission. This means that these monitors are not employed by the mission, but by their sending state. Security officers, however, are contracted directly by the mission. This is to ensure minimal conflicts of interest, and to enhance the trustworthiness of the security team.

As a consequence of this structure, the security department is not in command of the patrols or the actual operations. The security department has an advising role. There is, however, a large amount of cooperation with the operations department. On a more practical level, this means that the daily operations are being run by the operation department. They are the ones who do the tasking, but also the decision making in case of any emergency. The security department advises, but does not have any decision making power. The role of the security officers in the operational planning is the creation of security risk assessments (SRA). These SRAs are presented to the operations officers who will decide whether the patrol can commence or not. The outcome of the SRA is dependent on who is able to give security clearance for the patrol. When there is a low risk the patrol hub leader will decide, is there a medium level of risk, the team leader decides and in case of high risk the head of operations has to decide whether the patrol will go ahead. In the case of a patrol, where the risk is so high that an incident is imminent, the head of mission has to make the decision. The highest level of risk is less focussed on a single patrol, but more on the location of a patrol hub or the whole mission as such. In that case the organisation which commissioned the mission will decide, so in case of the OSCE SMM the permanent council of the OSCE would make that decision.

In practice, decision making works in the following way. Head Quarters decides to achieve a certain strategic goal. In that phase the head of operations will look at how to achieve that strategic goal on an operational level. The head of security will look at the plan, to see what kind of impact that might have on the safety and security of the staff. When the plan has been modified to minimise risk, the plan is passed down to team and hub level. Here is where the tactical decisions are made as to where the patrols should go, or whom to speak with. This is also where the hub security officer makes an assessment. The reason behind this is that this security officer is best placed to know the area and the people and can thereby make a proper assessment the threat. The plan goes back up to the team level, where the team operations will make a final decision. As we can see in the picture below, we can see that when the risk level is medium, the team leader can decide whether this patrol can commence.

This whole procedure has its roots in the ALARP principle. While any decision made or risk assessment produced may contain mistakes, it does not make sense for a Head of Mission has to give approval for every single patrol. Therefore, one can accept the risk of human error in the risk assessment, especially because it is minimised by several people looking at it.



*Figure 2: Respective risk and responsibility for go-ahead (2019)*

Security protocols and individual security measures are all recorded in so-called standard operation procedures (SOP). SOPs are written by either a planning cell or operation officers at the head office level. Documents like SOPs are normally written in cooperation with the staff in the field. It is common procedure that drafts are sent to the field for feedback. Only once this is done, an SOP is sent to the HoM, who will sign and approve it. Once this is done, the draft becomes an official SOP.

As such, we can say that the HoM is ultimately responsible for the security measures. Although it is up to every monitor individually to follow the SOPs and it is up to the operation officers to make sure that all the operative security measures are in place, in the end it is the HoM's signature under the proposed security measures.

## 5.2 How do the security measures which are in place work?

The purpose of the security measures is to minimise risks as far as possible. This is where the ALARP principle comes into play. Due to the nature of the work (monitoring compliance with peace agreements) the working environment can be very volatile. However, this does change from mission to mission. When we look at the EUMM Georgia, there has not been any confrontation between the (former) fighting parties since the peace agreement of August 2008.

This is in contrast to the Minsk agreements, which were intended to ensure a cease-fire in the conflict in the Donbass Area in Ukraine. According to the OSCE SMM bi-weekly report of 26 November 2018, just in those two weeks 11900 cease fire violations were observed (OSCE SMM, 2018). Even though the conditions vary, each mission always involves observing either a post-conflict situation, or a still active conflict. In addition, there are certain threats which are inevitable in conjunction with peace observation work. For instance, in the EUMM Georgia, most of the observation work is done close to the Administrative Boundary Line (ABL, this term is normally used for a de-facto borderline, which is not internationally recognized as an official border). However, when we look at the travel advice of the Ministry of Foreign Affairs of the Netherlands, we can see that for this area the advice is to travel there '*Only when absolutely necessary*' (Ministerie van Buitenlandse zaken, 2018). Visiting places such as these is an unavoidable part of peace observation missions, and as such will always carry the associated risks.

With the ALARP principle in mind, I would like to use the TEAR principle to assess the various security measures taken. The TEAR principle consists of four different methods to enhance security; transfer, eliminate acceptance and reduction of the risk. The transfer of risk is normally done by using insurance, in that way the (financial) risk is being carried by the insurance company. However, even insuring the lives of the monitors does not properly transfer the risk of the loss of life as such, and some vehicles and other equipment are too expensive to insure for it to be cost-effective. However, there are two significant ways in which this mission uses transfer of risk. One is the use of guards in the hotels and patrol bases. Placing (armed) guards outside these buildings transfers the initial risk of an attack on these buildings to the armed guards. One other is the use of a contracted long-range UAV (unmanned aerial vehicle) team. Initially the mission used their own assets for this, but due to the high risk of losing these UAVs, the difficulty to retrieve the lost UAVs and the high costs of these UAVs, these risks were transferred to a contracted company.

The elimination of risk is not possible; a risk-free environment would be an environment in which peace observation missions were not necessary. However, it may be possible to eliminate risk completely in contingency planning. For instance, when weather conditions are so bad that the risk becomes too high, all patrols will be cancelled. In this way, there is a complete elimination of the risk of traffic accidents due to bad weather. Also, if the general security risk becomes too high, then all operations or part of the operations can be cancelled.

There is an acceptance that the mission operates in an area where there is an increased risk; however it will never be accepted that human lives should be put in risk. The SOPs state clearly that there should not be, and that there is no reason to put one's life at risk. All SOPs state that there is nothing more important than the life of the monitors. The same is not true of mission assets. There is significant use of UAVs in the mission. Although there are various

mitigation measures in place, this does not always work and at least once every month a UAV is lost, and the fighting parties shoot at the UAVs at least once a week. This is accepted as this is the only way to monitor certain areas, and the financial impact is minimal.

Most of the efforts are put into reducing the risk to the assets and the personnel of the mission. This starts as soon as the staff is considered for selection. All monitors who want to apply to the mission must have a certain background. An unwritten rule in peace observation missions is that one third should have a military background, one third a law enforcement background and one third a civilian background. The military and police personnel have already received a certain amount of training in their original organisation. The civilian staff often has experience in previous missions or has had training from non-governmental organisations they have worked for. There are also several nations which have training programmes for their monitors. Finland, for instance, uses the Crisis Management Centre (CMC) in Kuopio. Once a monitor is hired, hostile environment awareness training (HEAT) is given to all new mission members. This is training to prepare the monitors for the actual situation they will be working in and is mandatory for all mission members. Once this is done there is also induction training, which is followed by more local training within the teams. All mission members follow this training regime.

Other measures are also in place, with most being instructions from SOPs. For instance, everybody who works within a certain distance of the front line has to wear body armour and a helmet. Also, the use of armoured vehicles is mandatory within a certain range of the contact line.

Perhaps one of the measures with the biggest influence is that monitors are only permitted to travel on paved roads. Due to the nature of the conflict in question, there is an extremely high density of unexploded ordnance (UXO) and mines. By only using paved roads, the risk of not seeing an UXO or the chance of triggering a mine is significantly lower.

It is also important for a peace observation mission that there is good contact with the fighting parties. Although a mission like this is always invited by the host nation, which is usually one of the parties to the conflict, there will always be at least one other party as well. When we look at the OSCE SMM, according to their website, there are three official parties; on one side the Ukrainian Government, and the other side the Luhansk Peoples Republic (LPR) and the Donetsk Peoples Republic (DPR) (OSCE, 2018). To be able to operate at the frontline, it is vital to make sure that all sides respect the status of the monitors as being impartial, and that they are not considered a threat. To create and sustain this feeling amongst the parties clear and open communication through liaison officers is of utmost importance. By doing this, the risk of being targeted by the parties is decreased.

### 5.3 How do the security measures influence the work of the monitors on the ground?

Because the only product of a peace observation mission is its reports, it is difficult to say how big the influence of security measures is on this work. One cannot say for certain whether security measures increase or decrease either the quantity or quality of the reports. However, I have experienced the measures myself as a participating observer, and have seen where operational needs conflicts with the security measures. The security measure limits the time of the monitors of how long they can stay in the field. Therefore the observations are only during a certain timeframe. Also only a small amount of the villages are accessible, so the monitors cannot see the impact of the conflict everywhere.

The body armour, which is worn by the monitors, is around fifteen kilograms. Although it only has to be worn within five kilometres of the frontline, most of the work is within this range. This is the area where the fighting takes place, so this is also where the monitors need to be present. We can see here how the ALARP principle has been used. Body armour is not required everywhere, but only in those places where the risk of harm is most acute. Wearing the body armour is a mitigation measure, as per the reduction element of TEAR. This type of body armour protects the wearer against small arms fire, and thus reduces the chance that the monitor would be injured by bullets or shrapnel.

During my time on the mission I had to wear the body armour for roughly six hours a day. This combined with the fact that the armoured vehicles have a less comfortable suspension system, and the condition of the roads, makes for very physically gruelling work. The physical stresses of this protective equipment have caused injuries to monitors in the past. It is particularly difficult when monitors have to observe a short-term cease-fire. This means standing outside and physically observing often in very inhospitable weather conditions, especially in summer with temperatures above 35 degrees. This makes the physical cost of wearing the armour even greater.

Most of the procedures which are described in the SOPs are time-consuming and require a lot of coordination. For instance, when patrols want to move within 5 kilometres of the front line, there must be another patrol on the other side. This requires coordination and communication between patrols, which is not always easy. Although the measures can be perceived as cumbersome, the monitors also understand that they are necessary; this communication is required to take control over the situation. By having control, one reduces risk. Although there is always a certain risk in a warzone, the ALARP principle shows that this mandatory communication is a worthwhile cost in exchange for a significant reduction of risk.

Road restrictions are by far the security measure with the greatest impact on the work of the monitors. The road conditions in the area of operations are very bad. Before the conflict the roads were already in quite bad conditions and the infrastructure in the area was not very

well developed or maintained. The conflict has only decreased the condition of the roads. This, combined with the security regulations, has a big impact on the reach of the monitors. The main roads are still driveable, but the roads and bridges closer to the frontline are smaller and in very bad condition. This means that there is a large group of villages and civilians who can't be reached. Of course, this is also known by the fighting parties, and is a fact often exploited to deceive the monitors. This also creates frustration in the monitors themselves, due to not being able to reach these civilian populations when other organisations do. Although these road restrictions come very close to a complete elimination of risk, it is still not total. Some mines are not meant to be put on the ground, and unexploded ordnance can be anywhere. However, even though the risk reduction is not absolute, and is not easily measurable, it certainly does reduce the risk a great deal. We know that before this measure, one vehicle was hit by an anti-tank mine, and since the measures came in place it has not happened. This is a positive indication, but is too little information from which to draw strong conclusions.

#### 5.4 Does using of the ALARP principle enhance productivity?

Productivity in peace observation missions is in general measured in two ways; the amount of patrols which are on the ground and the reports which are being sent out. On both of these measurements the ALARP principle has no influence on the number of reports produced or the number of patrols sent out. The patrols will be sent out in any case, and the amount of reports will stay the same. However, if the ALARP principle was used, the information gathered would be of higher quality and thus the reports would be better. By using the ALARP principle in the way as it should be used, the security measures can be tailor made for each patrol, instead of using a single security advice for the entire mission. If we take the OSCE SMM as an example, the regulations of not leaving hard surface, apply to the whole country and not only to the area where there is actual fighting. In the EUMM Georgia, similar rules apply.

## 6 Conclusions

It is clear from the above that, in general, the TEAR principle is being followed. Most of the measures noted above are focussed on reducing the risk. The transfer of risk is very limited, but these limits are well motivated. Insurance would be very costly and armed security personnel are only useable in certain locations (guards at certain forward patrol bases). Elimination of any risk is part of the SOPs. When the threat becomes too high, the operation can halt patrolling activity or even evacuate forward patrol bases or patrol hubs. Acceptance of risk is also in place. There are mitigation measures in place for various groups of risks, but there is also acceptance that not all risk can be eliminated. Almost all measures which are in place are purely focussed on mitigating the risk to the greatest feasible extent. From wearing body

armour to securing our supply chain of drinking water, all the measures have the goal of mitigating risk. There is a widespread understanding that there is no option of eliminating most risks, so bring it down to an acceptable level is the only good remaining option.

The ALARP principle is clearly being followed in these cases. By mitigating the risk as much as possible, the ALARP principle is being achieved. However, during my research I have realized that there are factors which could be of bigger influence than just security as such. When we look at the measure of not driving on unpaved roads, this decision was not made by the security department, or even advised by the security department. It was taken by the Head of Mission. There could be various reasons why the Head of Mission took this decision, but these are outside the scope of this research. However, it is a fact that this decision has been taken and been put in place, and it is worth noting that the security department is not the only source of such measures.

According to the factsheet of the OSCE SMM of 2017, that operation had deployed 25,914 patrols. One of these patrols was hit by an anti-tank mine, with a fatality as result. This is an occurrence of 0.0039% (If we look at a larger perspective, knowing that the mission started patrolling in the end of 2014, the percentage is even lower). When we look at the standards given by ISMI (2014a), this risk would score the lowest possible score of 1 on a 5 point scale. Even when we assess the impact as 5 (which is the highest grade) this would still give a low result on the risk assessment. That low risk does not justify a measure which is so far-reaching. Yes, the safety of the staff should always be the main priority; however this could also be done with more subtle measures. When we consider that this applies to the whole territory of Ukraine, instead of only the local area where there is a risk, the impact of the measure might be bigger than the actual risk is was. However, fatalities on such missions might also create geo-political tensions, which should be taken into account.

To finalize, I believe that the mission could work more effectively and efficiently by mirroring all SRAs and security measures against the ALARP principle. In general the principle is being used; however not really in the security planning. It is not being taken in consideration that there are differences in areas. A more flexible approach to the security measures would already increase the effectiveness. The ALARP principle should makes security officers think about what the needed security measures in a certain area are. It is very different if a monitor is operating in an area which is not affected by the conflict, than that the monitor is in an artillery bombardment. However, this is purely from a security and operation perspective. I did not take in consideration the political spectrum, which have a large impact on this as well.

## 6.1 Reliability and Validity

Reliability and Validity are two measures to identify the quality of research. Shah (no date) writes in his article regarding reliability and validity that the reliability of a research can be determined by addressing three questions. Firstly, when the research will be repeated in the same way, and with the same means, the outcome should be the same. Secondly, if the research is repeated by a different researcher, will the outcome be the same? Lastly, can a research with the same research question, but utilizing different methodology, be completed and achieve the same result? To measure the validity of the research, one must be able to answer the queries as to whether the employed measure actually measures the theoretical concept.

Robson (2002, 176) argues that there is a difference between quantitative research and qualitative research when addressing reliability. He states that reliability in qualitative research is more about “being thorough, careful and honest in carrying out the research.” The challenging issue with reliability and qualitative research, in particular with the participating observation method, is that the core of the research is a human observing other humans. This makes it nearly impossible to answer the three different questions Shah stated, in a positive way.

When we examine validity in qualitative research, Kriukow (2018) states the following in his article; “What seems more relevant when discussing qualitative studies is their validity, which very often is being addressed with regard to three common threats to validity in qualitative studies, namely researcher bias, reactivity and respondent bias.”

Kriukow (2018) describes the researcher bias as the negative impact the research can have on the input from the test group or even the research itself. Moreover, reactivity embodies the positive outcome the researcher can have on the research whereby respondent bias delineates how the test group responds to the researcher, either in a positive or in a negative way.

Robson (2002) outlines several different methods to mitigate the risk to these three threats. The author has utilized three of these. Firstly, the author used prolonged involvement. Robson claims that the longer the observer is part of the test group, the greater the likelihood that the test group will act in a natural way to the observer. Due to the fact that the author has been part of the test group for six months, and has been participating in all facets of the work, an atmosphere of trust and honesty has been created. However, Robson also writes that although the risk of the threat of researcher bias and respondent bias diminishes the risk of reactivity increases. Nonetheless, the author believes that this has not been the case with this research the author gains no benefit or disadvantage to the outcome of the research. To mitigate even further, the author has often used member checking. In other words, the researcher verifies with the test group whether the findings and the conclusion truly reflect what the test group experiences. Due to the close proximity to the test group, there was a

constant opportunity to validate the findings with the test group. According to Robson (2002), the risk lessens for all three threats when one uses this method. Finally, the author also employed negative case analysis. As such, particular members of the test group would always support their employer or the organization, for various reasons. Although it is easy to dismiss their opinion, it is prudent to investigate and research their perspective in each instance. The author spent quite some time following up on their view. According to Robson (2002) this reduces the threat on researcher bias.

## 6.2 Further research subjects

In the opinion of the author, this research should be followed up with a larger research. This should be done within one mission, but preferably within several missions or within one of the governmental organizations which establish missions (like the EU, the OSCE or the UN). The author also believes that it would be good to undertake a comparative analysis of different types of mission, for instance, a capacity enhancement mission and/or a security sector reform mission.

It is the opinion of the author that the most valuable would be to undertake a research on a far larger scale between different organizations or companies who operate in hazardous environments. There are numerous commercial companies and NGOs who operate in the same areas as these missions. It would be extremely beneficial if these different sectors would collaborate and learn from their respective best practices.

## References

- Aven, T & Jones-Lee, M. 2011. ALARP - What does it really mean? *Reliability Engineering & Systems Safety* 96 (8), 877-882.
- Aven, T. & Abrahamsen, E. 2006. On the Use of Cost-Benefit Analysis in ALARP Processes. *International Journal of Performability* 3 (3), 345-353
- Blyth, M. 2008. *Risk and Security Management*, Wiley, Hoboken, NJ.
- Broder, J. 2006. *Risk Analysis and the Security Survey*, Elsevier, Boston, MA.
- Calhoun, C. 2002. *Dictionary of the Social Sciences*. Oxford: Oxford University Press.
- DeWalt, K. M. & DeWalt, B. R. 2002. *Participant Observation: A Guide for Fieldworkers*. Walnut Creek: AltaMira Press.
- DeWalt, K. M., & DeWalt B. R. 2010. *Participant Observation: A Guide for Fieldworkers*. 2<sup>nd</sup> Edition. Walnut Creek: AltaMira Press.
- Gjerdrum D. & Peter, M. 2009. *The New International Standard on the Practice of Risk Management - A Comparison of ISO 31000:2009 and the COSO ERM Framework*, Society of Actuaries, United States
- Hardy, K & Runnels A. 2014. *Enterprise Risk Management: A guide for government professionals*. San Francisco: Jossey-Bass
- Hollinger R. 2017. *National Retail Security Survey 2017*, University of Florida
- ISMI. 2014a. *Security Risk Analysis*. Worcestershire, United Kingdom: The International Security Management Institute.
- ISMI. 2014b. *Security Design, Evaluation and Surveying*. Worcestershire, United Kingdom: The International Security Management Institute.
- ISO. 2018. *ISO 31000:2018*. International Standard Organisation
- Kovacich, G. & Halibozek, E. 2003. *The Manager's Handbook for Corporate Security : Establishing and Managing a Successful Assets Protection Program*, Elsevier Science & Technology.
- Mack N., Woodsong C., MacQueen KM., Guest G. & Namey E. 2005. *Qualitative research methods: a data collector's field guide*.
- Nichols, J. 2009. *Russia-Georgia Conflict in August 2008: Context and Implications for U.S. interests*, Congressional Research Service

OSCE SMM to Ukraine. 2018. OSCE SMM Status report of 28 November 2018, Organization for security and Co-operation in Europe.

OSCE. 1992. Treaty on Open Skies, Organization for security and Co-operation in Europe.

Raab, M. 2011. Concepts of Comprehensive Security, Austrian Institute for International Affairs

Robbins, A. 2003. Unlimited Power: The New Science of Personal Achievement, Google books.

Robson, C. 2002. Real world research: a resource for social scientists and practitioner-researchers. Oxford, UK: Blackwell Publishers.

Tardy, T. 2016. Civilian Crisis Management: Towards a new paradigm, European Union Institute for Security Studies.

Whyte, W. 1984. Learning from the field - A guide from experience. Beverly Hills: Sage Publications.

#### Electronic sources

EEAS. 2018. Common Security and Defence Policy. Accessed 12 January 2019.  
[https://eeas.europa.eu/topics/common-security-and-defence-policy-csdp\\_en](https://eeas.europa.eu/topics/common-security-and-defence-policy-csdp_en)

EEAS. No date. EU Border Assistance Mission in Libya (EUBAM) Accessed at 10 October 2018.  
[https://eeas.europa.eu/csdp-missions-operations/eubam-libya\\_en](https://eeas.europa.eu/csdp-missions-operations/eubam-libya_en)

EU. No date. European Union Monitor Mission to Georgia. Accessed 22 December 2018.  
<https://eumm.eu/>

Gowan, R. 2012. The U.N. Mission in Syria: Heading for Heroic Failure?, WPR. Accessed on 12 January 2019. <https://www.worldpoliticsreview.com/articles/11909/the-u-n-mission-in-syria-heading-for-heroic-failure>

IECEU. No date. Accessed on 11 December 2018. <http://www.ieceu-project.com/#home>

ISO. 2018. ISO 31000 - Risk management. Accessed on 12 September 2018.  
<https://www.iso.org/iso-31000-risk-management.html>

Krukow, J. 2018. Validity and reliability in qualitative research. Accessed on 9 May 2019.  
<https://qualitativeresearcher.me/2018/02/18/validity-and-reliability-in-qualitative-research/>

Melnikova, K. 2018. Peacekeeping mission in Donbass would mean an end to the republics. Accessed on 18 December 2018. <https://eadaaily.com/en/news/2018/02/21/peacekeeping-mission-in-donbass-would-mean-an-end-to-the-republics>

Ministerie van Buitenlandse Zaken. 2019. Reisadvies Georgie. Accessed on 06 January 2019. <https://www.nederlandwereldwijd.nl/reizen/reisadviezen/georgie>

Ministerie van Defensie. 1999. Minstriele- en defensiepublicaties. Accessed on 29 March 2019. [https://puc.overheid.nl/mp-bundels/doc/PUC\\_400100000002\\_10/1/](https://puc.overheid.nl/mp-bundels/doc/PUC_400100000002_10/1/)

Nieminen, L. 2017. Laurea's thesis guidelines. Accessed on 31 March 2019. <https://laureauas.sharepoint.com/sites/linken/Documents/Laurea's%20thesis%20guidelines.pdf>

OSCE. 2016. Spot Report by OSCE Special Monitoring Mission to Ukraine (SMM): SMM evacuates forward patrol base in Shchastia due to mortar shelling. Accessed 31 March 2019. <https://www.osce.org/ukraine-smm/261796>

OSCE. 2017. Nagorno-Karabakh conflict settlement: OSCE Chairmanship welcomes fresh commitment by Presidents of Armenia and Azerbaijan. Accessed on 04 January 2019. <https://www.osce.org/chairmanship/350416>

OSCE. No date. OSCE Mission to Georgia (closed). Accessed on 7 Jan 2019. <https://www.osce.org/georgia-closed>

OSCE. 2018. Special Monitoring Mission to Ukraine Accessed on 04 January 2019. <https://www.osce.org/special-monitoring-mission-to-ukraine>

Reilly, K. 2015. Shoplifting and Other Fraud Cost Retailers Nearly \$50 Billion Last Year. Accessed on 17 October 2018. <http://time.com/money/4829684/shoplifting-fraud-retail-survey/>

Robinson, M. 2009. U.N. monitors leave Georgia, OSCE mission shuts. Reuters. Accessed 9 Jan 2019. <https://www.reuters.com/article/us-georgia-monitors-idUSTRE55T3OR20090630>

Shah, D. No date. Reliability and Validity. Accessed on 9 May 2019. <https://dshah.journalism.wisc.edu/files/Reliability-and-Validity.pdf>

UN. 2013. UNSMIS. Accessed on 2 March 2019. <https://peacekeeping.un.org/mission/past/unsmis/>

UNIAN. 2017. Ukraine's envoy estimates costs of UN peacekeeping mission in Donbas at least 1 billion a year. Accessed on 19 December 2018. <https://www.unian.info/war/2117654-ukraines-envoy-estimates-costs-of-un-peacekeeping-mission-in-donbas-at-least-1-bln-a-year.html>

University of Southern California. 2018. Organizing Your Social Sciences Research Paper: Theoretical Framework. Accessed on 9 Nov 2018. <https://libguides.usc.edu/writingguide/theoreticalframework>

Wintour, P. 2018. ICRC pulls foreign staff out of Yemen, The Guardian, accessed on 31 March 2019. <https://www.theguardian.com/world/2018/jun/07/icrc-pulls-foreign-staff-out-of-yemen>

## Figures

*Figure 1: CCM Command Structure (2019)* ..... 24

*Figure 2: Respective risk and responsibility for go-ahead (2019)* ..... 26