Aid Worker Security in Conflict Areas

On the Role of Technologies and the Use of Remote Management

Abstract

This research describes the various and complex ways in which technological developments affect aid agencies' security strategies, including their use of Remote Management (a security strategy in which international aid workers are removed from the field while national aid workers or national partners implement projects on the ground). After conducting interviews with representatives of the ICRC, NGOs and the UN in Afghanistan, Iraq, Somalia, South Sudan and Syria, this research compares and explains their security management strategies, their approaches to technologies and their implementations of Remote Management. As an exploratory study on this topic, it demonstrates that the rise in the use of technologies improves the aid sector's protection strategies and allows international aid workers to conduct an increasing number of tasks from a remote location (enabling Remote Management). Although views on Remote Management are ambiguous and reserved, information and communication technologies significantly reduce its challenges. The increasing usage of technologies and Remote Management in the aid sector can be explained and criticized by using social science theories of Beck and Foucault as well as theories on the increasing remoteness, politicization, militarization and commercialization of aid delivery. Regardless of the critiques, due to the practical benefits and opportunities of technologies, technological tools can be expected to be increasingly used in the aid sector's security management and, therefore, Remote Management will most certainly remain a popular strategy for the years to come.

Jori Kalkman
920113416040
Dr. Bram Jansen
Master International Development Studies
Sociology of Development and Change
Wageningen University

Executive Summary

This research aims to describe the various and complex ways in which technological developments affect the security management strategies of aid agencies in conflict settings. It specifically focuses on how technologies improve the security of international staff members by enabling Remote Management, a security strategy in which international staff manages an aid project from a remote (and secure) location while national staff or national partners implement projects on the ground. The main research question is therefore formulated as: *How do technological developments affect the security management of aid agencies as well as their views on and their implementations of Remote Management*? In order to understand and explain this question, this research, first, discusses aid agencies' risk perceptions and security management strategies, second, elaborates how technologies are used to improve aid worker security and, third, shows how the use of technologies leads to Remote Management.

A study of the scientific literature has been carried out to explore the concepts of this research and to contextualize and explain the empirical findings. In addition, humanitarian reports (i.e. grey literature) have been studied in order to find out which role technologies play in the aid sector and how aid agencies manage their security in volatile settings. The main source of information, however, were 31 interviews with security managers, country directors and experts, which were conducted over a period of five months (December 2014 - April 2015) and were afterwards transcribed and coded. This research focuses specifically on aid agencies (ICRC, NGOs and UN) in Afghanistan, Iraq, Somalia, South Sudan and Syria.

In general, technologies in the aid sector prove to be highly beneficial in terms of efficiency, effectiveness, visualization and democratization. Nevertheless, technologies are not generally accepted by all parties to a conflict. Some conditions for the implementation of technologies (e.g. sufficient education) tend to lack in conflict settings as well. Moreover, there is fundamental skepticism with regard to the effects of technologies on power relations and the reliability of data. Since aid agencies find ways to deal with these challenges, it is almost beyond doubt that the role of technologies in conflict settings will increase. A worrying trend, however, is that threat sources (e.g. armed groups and criminals) are using technologies more and more as well, which increases the perceived risks.

Aid agencies in Somalia and Syria tend to view risks as higher and more diverse than elsewhere, which explains the increased use of deterrence and protection strategies in these countries. In South Sudan and Iraq, on the other hand, the main risk is perceived to be collateral damage, which leads aid agencies to mostly use acceptance strategies. The UN consistently sees risks as higher and therefore resorts more often to protection and deterrence, whereas the ICRC sees situations generally as less threatening and is more likely to use acceptance measures. NGOs report very diverse views, but an expected distinction between humanitarian and development NGOs did not prove fruitful. A distinction that could be drawn, however, is the distinction between religious and other NGOs, with Christian NGOs being slightly more at risk in Islamic countries. In general, however, all NGOs rely mostly on protection measures in the countries under study.

In their security management, aid agencies have begun to make use of technologies. For instance, agencies reported the usage of new security information-gathering tools and tracking devices as well as security information-sharing tools and online security trainings. There are also various technologies that improve aid worker security indirectly by reducing the need for (international) staff to be in the field (e.g. satellites, drones and online cash transfers). Of course, this reliance leads to new vulnerabilities against which aid agencies need to protect themselves. While the ICRC and the UN have conducted some large-scale technological projects, the introduction of relatively basic technological tools is somewhat lagging behind in comparison with NGOs. In general, technologies are not yet used at a very large scale in conflict settings, but they are being progressively introduced in even the most volatile settings.

The process of an increasing use of technologies by aid agencies has enabled Remote Management (defined as: 'a mode of operation in which international staff, either after relocation, after evacuation or by design, manages a project from a distant location because of high or increasing security risks, while national staff members or local partners implement the project on the ground'). Strikingly, agencies in countries in which this strategy has a long history are more critical than agencies in countries in which it has been adopted recently. Also, headquarters' staff is slightly more positive than field-based staff. It is worrying that few agencies know how their national staff perceives Remote Management. Nevertheless, the widely accepted view on Remote Management as a morally questionable transfer of risks from internationals to nationals can be nuanced by pointing out that risks are not actually 'transferred', while the morality of changing risk profiles in Remote Management is not necessarily morally questionable either.

Remote Management is used in all of the conflict settings studied in this research by almost all of the agencies that were interviewed. The higher risk perceptions in Syria and Somalia have led to a more widespread use of Remote Management and the withdrawal of internationals abroad (instead of to a safer region in the country). Next to working through national staff and working through national implementing partners, various innovative alternatives have been designed and implemented, especially in areas in which aid agencies have used the strategy over an extended period of time. The availability of technologies has significantly reduced the negative ramifications of Remote Management on planning, communication between staff members, the security of national implementers and the ability to monitor. In short, technologies have made Remote Management much easier and more effective.

On the basis of social science theories, it is possible to criticize the aid agencies' resort to technologies and Remote Management for various reasons. For instance, from a Foucauldian point of view, it can be argued that technologies simply enable aid agencies to control populations (i.e. beneficiaries) and staff members better. Taking a Beckian perspectives, the aid sector has become fundamentally risk averse and will have to update its technologies constantly to prevent failures. Also, it can be claimed that Remote Management and technologies have negative effects on the aid sector at large by politicizing aid (through shifting the decision-making to Western centers of power in the global South), by militarizing aid (which raises questions on how aid agencies should position themselves in conflicts) and by commercializing aid (through blurring the lines between aid and business activities). A final point of critique is that Remote Management and technologies socially, emotionally and psychologically detach international staff from the field, which has negative repercussions for the nature and quality of aid provision. Although these claims may overstate the challenges ahead somewhat, it is beyond doubt that the aid sector faces some pressing questions which are worthwhile studying and debating.

Contents

Abbreviations

DFID	Department for International Development (UK)
ECHO	European Commission's Humanitarian Aid and Civil Protection Department
GIS	Geographic Information System
GPS	Global Positioning System
ICRC	International Committee of the Red Cross
ICT	Information and Communications Technology
IDP	Internally Displaced Person
IED	Improvised Explosive Device
IFRC	International Federation of the Red Cross
INGO	International Non-Governmental Organization
INSO	International NGO Safety Organization
ISIL	Islamic State in Iraq and the Levant
M&E	Monitoring and Evaluation
NGO	Non-Governmental Organization
NSP	NGO Safety Program (Somalia)
SBTF	Standby Task Force
SMS	Short Message Service
UAV	Unmanned Aerial Vehicle
UN	United Nations
UNDP	United Nations Development Programme
UNDSS	United Nations Department of Safety and Security
UNHCR	United Nations High Commissioner for Refugees
UNMISS	United Nations Mission in the Republic of South Sudan
UNOCHA	United Nations Office for the Coordination of Humanitarian Affairs
UNOSAT	United Nations Operational Satellite Applications Programme
VTC	Video Teleconferencing
WFP	World Food Programme

Glossary

Acceptance	A security management strategy, which aims at reducing risks to aid agencies through building good relationships with relevant stakeholders, such as local communities and authorities
Aid agency	Non-profit organization with humanitarian goals (in this research specifically: UN, ICRC and NGOs)
Big Data	Advanced computing tools and methods that are used for analyzing huge amounts of collected data (in lowercase letters: the collected data itself)
Communication Technology	Technologies that can be used for communication purposes
Conflict setting	Environments in which violent conflict is regular and protracted (in this research specifically: Afghanistan, Iran, Somalia, South Sudan and Syria)
Crowdsourcing	The production of information by a (usually online) community, varying from reporting to processing information
Deterrence	A security management strategy, which aims at reducing risks to aid agencies through posing a counter-threat
International staff	Aid agency staff member that is not a national to the country of operation (also: expatriate staff)
Information Technology	Technologies that can be used for information-gathering purposes
National staff	Aid agency staff member that is a national to the country of operation
Protection	A security management strategy, which aims at reducing the vulnerability of aid agencies by adopting devices, materials and procedures
Remote Management	A mode of operation in which international staff, either after relocation, after evacuation or by design, manages a project from a distant location because of high or increasing security risks, while national staff members or local partners implement the project on the ground
Risk	The possibility or probability of a negative consequence
Risk perception	The subjective estimation of the possibility or probability of a negative consequence
Security	The freedom from risk and harm resulting from violence and other acts
Security management	The attempt to reduce exposure to the most serious risks by identifying, monitoring and tackling key risk factors (also: risk management)
Technology	The use of (scientific) knowledge for practical ends
Threat	A danger in the operating environment

Chapter 1: Introduction

Problem statement and research questions

The reported number of violent incidents against aid workers has risen exponentially over the last decades. Stoddard et al. (2009) reported an increasing number of attacks on aid workers in the period 1997-2008, while the latest Aid Worker Security Report shows an unprecedented high number of incidents (Stoddard et al., 2014). Since 2006, there have been more than 200 aid worker victims annually and an all-time high of 460 aid worker were victimized in 2013 (see figure 1). Both reports mention that most of the incidents took place in a few highly volatile settings, which include Afghanistan, Pakistan, Somalia, South Sudan, Sudan and Syria. Attackers did not discriminate between aid agencies. Aid workers of the United Nations (UN), employees of the International Community of the Red Cross (ICRC) and staff of Non-Governmental Organizations (NGOs) were targeted alike. In addition, both national staff and international staff fell victim (Ibid.).

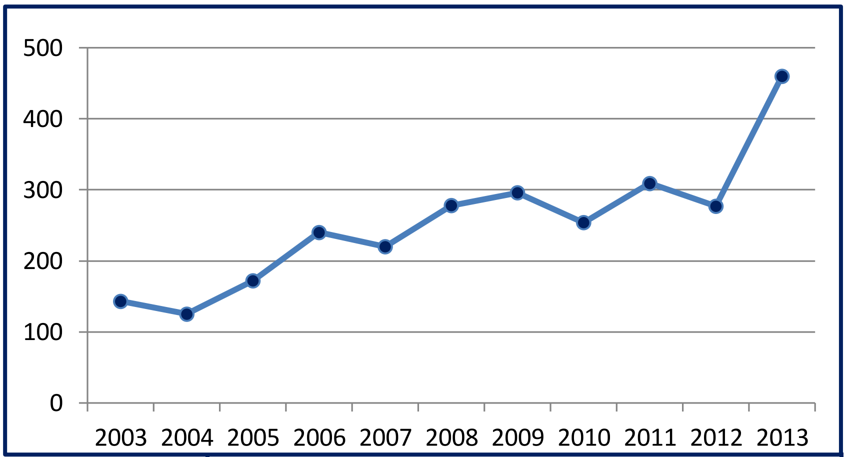

Figure 1: Aid worker victims (2003-2013) (Stoddard et al., 2014)

With an increasing number of reported incidents, aid agencies are called to improve the security of their staff. Historically, the preferred security strategy is building acceptance (HPN, 2010). If the community accepts the aid agency's presence, the members of the community will not target or threaten its staff. However, this strategy is often insufficient. The acceptance of a local community is unable to protect aid workers against the unintended consequences of large-scale artillery attacks, Improvised Explosive Devices (IEDs) and military standoffs. Since military equipment allows armed actors to attack groups of people from a large distance (e.g. through airplanes) or even without having to actively pull a trigger or push a button (e.g. IEDs), aid workers are also more likely to become accidental victims (i.e. collateral damage). Therefore, aid agencies make increasingly more use of protection strategies.

The implementation of security measures aiming to reverse the trend of rising numbers of aid worker incidents is influenced by technological developments in various and complex ways. On the one hand, technological developments allow belligerent parties to use more destructive force and to spread their propaganda more effectively. On the other hand, innovations enable aid agencies to improve their staff security by using better data-gathering techniques and by upgrading protection measures. Moreover, technologies reduce the need for staff to be physically in the field. International staff members, which are often perceived to be at higher risk, can more therefore be removed to safer, distant locations, from where they manage and oversee project implementation through new, advanced modes of information-sharing and communication. This strategy, called Remote Management, has become increasingly popular and is specifically used in areas that are deemed too dangerous for international aid workers (Stoddard et al., 2009, 2010).

In summary, aid agencies are faced with a complex interplay of rising (reported) incident numbers, failing traditional security strategies and the development of new risk-reducing measures, such as new uses of technologies and Remote Management. This begs the question how exactly aid agencies' use of technologies lead to the choice for and implementation of Remote Management as a security strategy. Questions that need to be addressed, as part of this bigger question, focus on how technologies influence security strategies and how Remote Management relates to existing security strategies as well as how aid agency representatives view concepts as security, technologies and Remote Management.

Research objectives

This research aims to clarify and disentangle the various effects of technological developments on the aid sector's management of risks and its use of Remote Management. In order to unveil these effects, several sub-questions are to be answered. Firstly, this research sets out to discover how aid agencies perceive the threats and risks in the environments in which they work and which security strategies they employ to tackle or mitigate these risks.

Secondly, with the rise of more advanced and cheaper technologies, the way in which aid agencies try to mitigate and manage risks has changed. New modes of information-gathering and improved communication tools are integrated in the security strategies of aid actors. This research aims to study which technologies are being used in the security management of aid agencies, how they affect aid delivery and how they lead to Remote Management.

Thirdly, with the practice of Remote Management becoming increasingly popular, it is worthwhile to find out how aid agencies think about managing projects remotely. Their view on Remote Management influences how easily aid agencies switch their *modus operandi* to Remote Management. In addition, the implementation of Remote Management, including the challenges, benefits and variants that aid agencies mention, will be highlighted in order to demonstrate what aid agencies find important in aid delivery in a remotely managed project and how they implement technologies in their use of Remote Management.

The objectives of this research can therefore be summarized as follows:

1) To find out how aid agencies perceive the risks in their environment, which security strategies they use and how the risk perceptions relate to the chosen security strategies.

2) To study which technologies are being used for security purposes and to scrutinize the effects of technological innovations on the security management of aid agencies as well as how technological progress facilitates or enables their use of Remote Management.

3) To discover how aid agencies view Remote Management and how they implement remotely managed projects, including which challenges they face and which technologies they use in these projects.

Social and scientific relevance

Fast (2010) argued that there is an epistemic gap in the literature on aid worker violence. While some writers on the issue use an 'epidemiological approach' by gathering incident data and analyzing 'proximate causes', others focus on the 'deep causes' and almost refrain from using any practical evidence (Ibid.: 367). The former group of scholars deals with very specific cases and aims to explain these, whereas the latter group assumes a rise in aid worker victims and applies very abstract theories and concepts to explain this rise. Thus, Fast (2010) claims, there is a gap between theory and practice in the writings on this issue.

There is a similar epistemic gap in the literature on aid agencies' risk management. This gap is created by the very diverse views and goals of the writers on this issue as well. Comparable to Fast's first group of authors, some writers on aid agency security management take a very practical stance, prescribing appropriate security strategies and providing guidelines. These authors use their interpretations of causation and solution on the basis of case-to-case evidence. A second group of scientists, which is very similar to the latter group of scholars that Fast refers to, is virtually always using very abstract theories and tends to use 'deep causes and consequences' for explaining aid agencies' security management strategies. Although it is hard to avoid joining one of these groups in the analysis of this research (especially due to the novelty of the topics at hand), this research will try to avoid using the newly acquired data for merely discussing either the proximate or the deep explanations by, instead, taking a 'middle ground'.

By only looking at the proximate or the deep explanations, explanatory theories have limited value since relevant information is neglected. For instance, the group of writers that only looks at the proximate explanations overlooks trends and patterns. This renders it impossible to explain how aid agencies use Remote Management or technologies *in general* as well as why aid agencies choose for a specific security management system. Just as Fast noticed, the other group of writers, by (almost) solely focusing on (global or societal) trends, tends to be detached from the 'real world' due to a strong reliance on anecdotal and contextual evidence and portrays aid agencies as passive actors, both of which limit the practical relevance of the theories. As Fast (2010: 382) argues: 'the problems and solutions are multiple and complex, involving a range of deep and proximate causes'.

Therefore, this research will provide explanations for the empirical findings, while embedding the research in social science theories, relating the evidence to some of the fundamental trends and adding scientific remarks throughout the chapters. It aims to not only share information on issues in which factual information is scarce (e.g. the role of technology in the aid sector), but it also tries to draw comparisons between types of aid agencies (the UN, the ICRC and NGOs) and between countries (Afghanistan, Iraq Somalia, South Sudan and Syria) in order to go beyond the mere sharing of best practices. Thus, by including both proximate and deep explanations as well as by exploring how they relate, this research aims to prevent falling in the trap of only adding to one of these approaches. The combination of unstudied phenomena (e.g. technologies in aid agency security management) and the use of the 'middle ground' approach make the research scientifically relevant.

In addition, this research tries to be socially relevant. With both the continued rise in reported aid worker victims and with the continued attempts of aid agencies to find ways to stay, it is important to see how security management and Remote Management are affected by technological progress. By studying how aid agencies use technologies to improve the security of their staff and by scrutinizing Remote Management as a security management strategy, successful risk mitigation measures and Remote Management practices will come to the fore which can help aid agencies to start or expand their activities in areas under threat. Also, since the middle ground approach aims to provide a richer understanding of aid agencies' risk management, this research hopes to contribute to the formulation of appropriate security strategies. The final report will therefore be disseminated among aid agencies.

Research questions and structure

Based on the problem statement and the research objectives, the main research question is defined as follows:

> *How do technological developments affect the security management of aid agencies as well as their views on and their implementations of Remote Management*?

Before diving into this question, the main actors of this research and the methodological approach will be elaborated in the remainder of this chapter. The second chapter will provide the theoretical framework, highlighting the main concepts and scientific theories. Since technology is the major concept in this research, its use, limits and potentials are discussed in chapter three. Chapter four outlines the risk perceptions of aid agencies and the traditional security management strategies that aim to tackle these risks. Subsequently, the use of technologies in the security management of aid agencies and its effects are addressed in chapter five. The sixth chapter introduces the views on Remote Management whereas chapter seven describes the implementation of remotely managed projects. Chapter eight, finally, provides the conclusion and discussion of the research.

Actors

Aid agencies are the key actors in this research. Their security management approaches, their use of technologies and their implementations of Remote Management are essential elements of this study. The aid sector at large has its own culture with some distinct features. For instance, aid workers have their own discourses (including words as capacity-building), their own micro-applications (e.g. the Millennium Development Goals) and their own worldviews (Apthorpe, 2011). Coining this reality 'Aidland', Apthorpe (2011) acknowledges that, regardless of these common characteristics, aid agencies also have their own culture, depending on their mission, mandate, goals, size, services and history, which all affect how aid workers look at and act in the world (Ibid.: 204).

In this research, the term 'aid agency' includes all non-profit organizations with humanitarian goals, but it specifically refers to those agencies providing humanitarian or development goods and services in the conflict settings under study. Since there is a multitude of views, it is worthwhile comparing different types of aid agencies and finding out how different organizational cultures lead to different views and actions (see Ibid.). The first distinction that can be drawn is the distinction between the ICRC, NGOs and the UN. These three groups, though all inspired by the humanitarian imperative, have very different cultures, missions, legal positions, goals and histories and, consequently, face divergent risks and use varying security management approaches.

Next to being an aid organization through, for instance, the United Nations Office for the Coordination of Humanitarian Affairs (UNOCHA) and the United Nations Development Programme (UNDP), the United Nations is also inherently a political organization with its own agenda and goals. After the 2003 attack on its Baghdad offices, the UN founded the United Nations Department of Safety and Security (UNDSS), which is tasked with the security management of the UN system (Collinson and Duffield, 2013).

The International Committee of the Red Cross and its national counterparts (i.e. the National Red Cross and Red Crescent Societies) are, as laid down in international law, legally mandated to act in cases of international and national armed conflicts (ICRC, 2015). The ICRC is therefore very different from other NGOs. To enhance its security, the ICRC seeks to negotiate access through dialogues with the parties involved and stresses its purely neutral standpoint in any conflict. Because of its apolitical neutral nature, the ICRC also refrains from speaking out against (violent) actors (Stoddard et al., 2009).

The NGO sector is very diverse in itself. It includes large international NGOs and small local ones. In addition, their task, mandates, views and missions are highly variable (Stoddard, 2003a). In this research, the focus will be on international NGOs (INGOs), usually based in the United States and Europe, since they account for the largest share of the humanitarian and development aid provided in conflict settings (Ibid.). Their diversity allows for a broad array of security management approaches, uses of technology and Remote Management experiences.

NGOs can be distinguished on the basis of their approaches to security questions. Stoddard et al. (2003a) and Metcalfe et al. (2011) make a distinction between two types of NGOs. Firstly, there are humanitarian agencies, which aim to strictly comply with the humanitarian principles and try to distance themselves from governments. These agencies rely on acceptance-building measures for security and can be expected to perceive risks as lower. Secondly, there are multi-mandated agencies, which are not only providing aid but are (also) tasked with spreading Western values and are more strongly linked to (Western) governments (Ibid.). This group of agencies can be expected to perceive risks as higher and is more willing to use protection and deterrence measures in order to 'secure' their agenda. Admittedly, this distinction oversimplifies reality somewhat. A clear line between humanitarian and multi-mandate agencies cannot be drawn since many agencies combine aspects of both. However, the distinction could be seen as a scale in order to allow for relative comparisons. This would mean that (more) humanitarian agencies are prone to use acceptance strategies, while their multi-mandated counterparts are likely to (also) employ protection and deterrence strategies.

Individuals within aid agencies

Aid agencies are not uniform. They are huge entities, in which individuals are (partly) responsible for (country) security management and the management of programs and projects. Multiple individuals within aid agencies are therefore relevant to this research. The most senior managers in a country are the country directors. Although strongly relying on the (local) expertise of other staff members, they are usually responsible for the final decisions on security strategies, while they are also central in managing critical incidents. In addition, they have the final responsibility for the (operational) structure of a program or project (HPN, 2010). Although they may devolve tasks, they are relevant since they hold the primary responsibility for their agency's activities.

Many international NGOs, especially the bigger ones, have security managers, also known by a variety of other titles, such as security focal points, security advisors and safety managers. In smaller NGOs and at headquarters' level, security is often one of the tasks of a staff member, which is combined, for instance, with logistics or operations. Being responsible for the daily management of security, the security manager is usually tasked with doing risk analyses, advising on security strategies, managing security officers, briefing and training staff, maintaining an incident database and assisting during critical incidents (Ibid.).

Of course, other staff members are involved in security management as well. First and foremost, all staff is responsible for their own (and other staff's) security (Candy, 2014). Security cannot be a single person's responsibility but is a collective endeavor. In addition, security policies, accountability structures and general guidelines, impacting security management practices on the ground, are usually adopted at the headquarters' level (HPN, 2010). Moreover, security strategies, such as Remote Management, affect program design, costs and monitoring activities. Thus, security strategies influence staff working in many different departments. Lastly, next to the effects of security strategies on international (decision-making) staff, national staff may be burdened with additional risk management tasks, especially in areas that are hard to access (Stoddard et al., 2010).

Other actors

There are a few other actors that affect either the aid sector's risk perception or its security management. Firstly, there are actors who cause or pose the risk. Belligerents in a conflict may accidentally kill or wound aid workers. Although data on the number of unintentional victims is very scarce, Sheik et al. (2000) reported that in the period 1985-1998, about a third of the aid worker deaths were caused by a combination of unintentional causes (including car accidents and diseases). These accidental cases may affect the perceptions of risks and therefore the aid sector's response.

In addition to unintended violence against aid workers, aid agencies are frequently targeted. For instance, militant Jihadist groups are perceived to have started an all-out war against the West (Canter and Sarangi, 2009), exemplified by the beheadings of aid workers by the Islamic State of Iraq and the Levant (ISIL). Furthermore, armed groups are believed to target the aid sector because aid has become a means for Western political or security interests or is seen as intrinsically Western (Collinson and Duffield, 2013; Egeland et al., 2011; Stoddard and Harmer, 2010). Lastly, local-political reasons and the wealth of aid agencies can lead to violence by, respectively, local opposition groups and criminals (Abild, 2010; Gundel, 2006).

As a final category, there are actors who influence or mediate the security management of aid actors. Firstly, governments and local authorities affect the project, for instance when they only allow national staff to operate in a specific area or when they determine which (security) tools can be imported. Secondly, donors, by their selective donation of grants, influence which projects are implemented and can exercise influence in this way over the implementation of projects (Costa, 2012). Donors can also ask for security plans or fund aid worker security projects. Lastly, NGO forums have been established to, amongst others, improve security information-sharing and security collaboration among NGOs. They usually provide statistics and analyses on security incidents and trends and they organize security trainings for NGO staff (see e.g. NSP, 2015).

Methodology

The objective of this research was to reconstruct the views on and implementation of aid agencies' security management strategies and, in particular, Remote Management by highlighting the role of technological developments. Since agencies are very different in their nature, goals and mandates, the interpretations of concepts such as 'risk' and 'security' were very different as well. As a consequence, the social meanings that individuals ascribed to the main themes in this research were subjective and variable. At the same time, these social meanings were the only source of information that could give information on how aid agencies view security management, how they look at technologies and what they think of Remote Management. The constructivist approach values the social, cultural and historical nature of the subjective constructions and allows for the inclusion of the multi-sided views of informants (Creswell, 2003). As such, it was the most appropriate paradigm for gathering and interpreting the information of this research.

Literature study

The first source of information for this research was the literature, both the academic literature of peer-reviewed scientific journals and the literature embodied in reports written for or by aid agencies. The academic literature was, first of all, a vital source of knowledge for the theoretical underpinning since this research builds on academic views on risk perceptions, security management, technologies and Remote Management. In addition, the ideas and views of social scientists proved necessary in order to be able to explain, analyze and contextualize the collected empirical data.

Furthermore, the grey literature was studied. Grey literature can be described in various ways, for instance as any literature that is hard to retrieve, as anything not published in peer-reviewed academic journals or even as any accessible literature that is not easily found in the most frequently used electronic databases (Rothstein and Hopewell, 2009). In this context, grey literature referred to anything that was published by or for aid agencies. The grey literature was a welcome addition to the scientific literature, because it reflected the views of aid actors on the topics studied in this paper. Since these articles were in general open-source documents, cautious and selective use was warranted. In short, articles, reports and guidelines by humanitarian consultants, think tanks, NGOs, NGO fora, UN bodies (e.g. OCHA), the ICRC and donors (e.g. ECHO) were used as sources of information next to books and articles of social scientists.

Interviews

The most important source of information for this research, however, were semi-structured, in-depth interviews. Conducting interviews is one of the most important tools of qualitative research and was particularly suitable for this research since the subjective constructions of reality are best captured through open-ended questions (Creswell, 2003). It is important to acknowledge that the researcher, just like the research population, constructs reality and thus reconstructed the constructions of the research population (Guba and Lincoln, 1994: 115). In other words, the researcher constructed a 'second-level narrative' (Borland, 1991). The goal of this research, following the constructivist line of thought, was to understand and interpret the views of the representatives of aid agencies. By creating more informed and sophisticated constructions of how they view security management, technologies and Remote Management, this research aimed to accumulate knowledge and, thus, attain scientific progress (Guba and Lincoln, 1994: 113-114).

The interviews for this research have been conducted between December 2014 and April 2015. A total of 31 informants have been interviewed for, usually, half an hour to an hour. The sample includes representatives of UN agencies (five interviews), ICRC delegations (four interviewees), NGOs (nineteen interviews) as well as a CEO of an aid worker security training company, a security manager at a Governmental Organization and an independent consultant on risk management strategies.

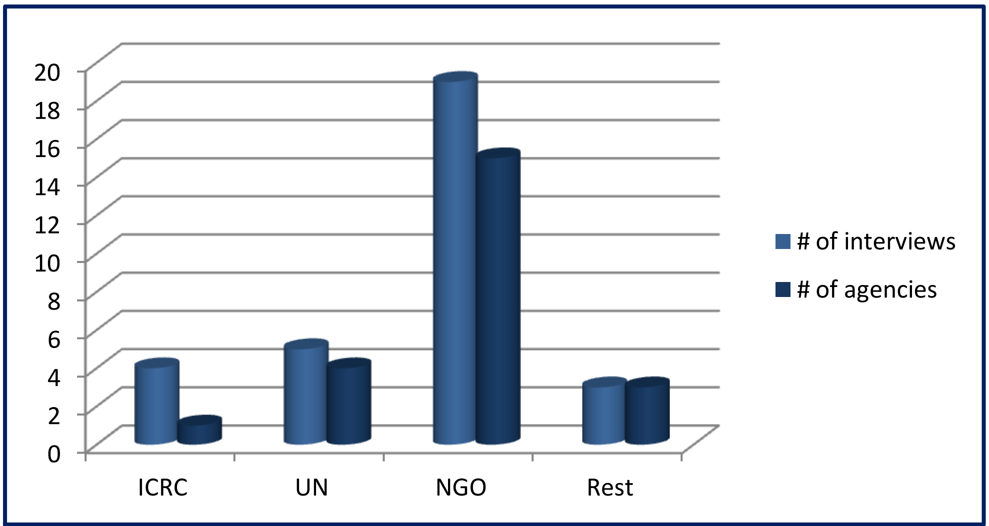

Figure 2: Background of interviewees

Most of the interviewees were tasked with the security policies of their aid organization. These interviewees have been grouped under the title 'security manager', although there were many alternative titles (e.g. security focal point, safety manager, security adviser and security field officer). The different titles were somewhat artificially applied since there were no clear definitions or boundaries, but the people holding these titles were united in their work on security issues for their agency. Due to financial or institutional reasons, some aid agency staff combined their security responsibilities with other tasks (labeled as 'combined tasks').

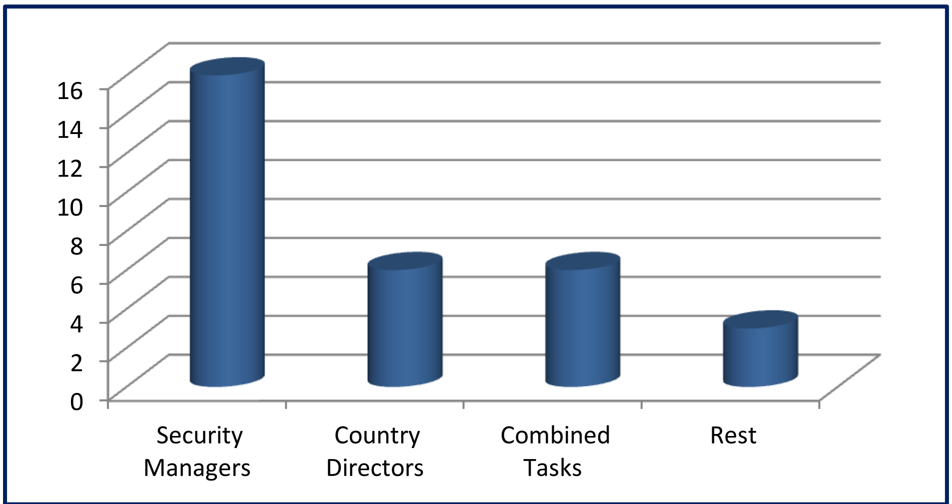

Figure 3: Roles of Interviewees

In order to study the effects of Remote Management on aid delivery and to get an insight in how technologies are used in other fields than security management, country directors have been interviewed as well. In addition, experts on risk mitigation proved interesting for this research to find out more about the security management of the aid sector at large and the different approaches to risks. Lastly, a head of technology from one NGO (Medair) has been interviewed to acquire some additional insights in how aid agencies view and use technologies.

This research is limited in the sense that only senior management staff members were interviewed. Of course, security policies are not solely determined by expatriate security managers and country directors but are negotiated outcomes in the social interface between national and international staff. However, since security policies are in the end adopted by the senior management (HPN, 2010), it is not primarily relevant to understand the views of national staff but rather how the expatriate security managers and country directors think that national staff views the issues of this research. Therefore, national staff members were not interviewed but interviewees were asked what they knew of the perceptions of their national staff.

Figure 4: Map highlighting the countries under study

Lastly, the interviewees were also selected on the basis of their geographical focus area. Since this research is about security management and the use of technologies for enhancing staff security, it was essential to interview staff in some of the most dangerous countries for aid workers. According to the last Aid Worker Security Report (Stoddard et al., 2014: 2), these countries were Afghanistan (with 81 attacks), Syria (with 43 attacks) and South Sudan (with 35 attacks). Somalia and Iraq were added to the sample, because of the frequency and scale at which aid agencies have used and use Remote Management in these countries. Lastly, some headquarters' security managers and independent experts were interviewed in order to, respectively, test the differences in views at different organizational levels and allow for comparisons between different countries. The list of interviewees, their employers and their geographical work areas can be found in Appendix I.

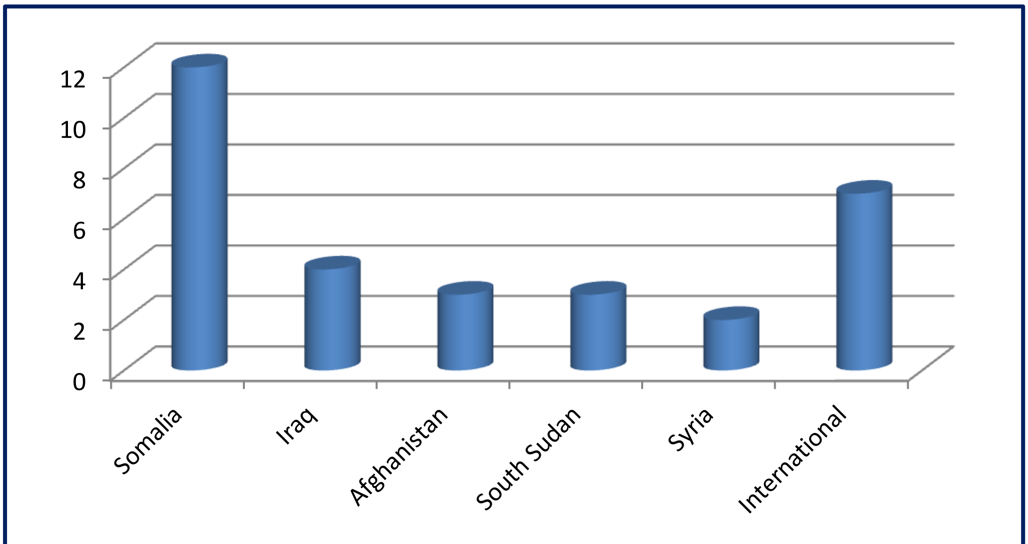

Figure 5: Geographical scope of interviewees

Skype-interviews

Apart from a few interviewees who preferred face-to-face interviewees and happened to be within travel distance (e.g. staff on leave), the utmost part of the interviews took place via Skype. As a free communication software, Skype (as a Voice over Internet Protocol) enables online video and audio calls between computers and other devices. Its use for research purposes only recently commenced and seems most vividly defended by PhDs, although they, as well, generally advise a serious evaluation of the match between the method and the research (Janghorban et al., 2014). Cater (2011) argues that Skype-interviews are particularly useful when participants are geographically dispersed and financial difficulties make face-to-face interviews (near to) impossible. Moreover, Skype-interviews are more time-effective, provide both interviewer and interviewee with more flexibility for making the appointment, render it easier for interviewees to withdraw and make assuring anonymity easier (Deakin and Wakefield, 2013).

In this research, Skype was particularly useful for a variety of reasons. Firstly, the locations of the selected interviewees were not only geographically dispersed but also difficult to access due to security reasons. Without Skype, interviews with aid workers in Mogadishu or Baghdad would have been impossible. Also, since security is a highly sensitive topic, Skype was a useful tool as it provides the interviewee with the ability (or power) to end the interview at any given moment. The decision not to use a webcam, which frequently happened, gave the interviewee some additional anonymity, enabling more honest conversations. In addition, many senior staff members were very busy and favored the flexibility of Skype, because it allowed for the postponement of interviews if necessary.

Another important reason for using Skype-interviews in this research was that the method fit the content of the research in a unique way. As this research focuses to a large extent on technologies, using technological tools for data collection seemed a more appropriate method than the old-fashioned way of data-gathering. Moreover, in Remote Management, Skype-interviews are an important mode of communication between international and national staff. International aid workers that have experience with Remote Management frequently talk with their colleagues or with contractors just as I talked with them. This mode of communication may therefore even be more familiar to them than work-related face-to-face conversations, which are rare in Remote Management projects. Although not being in their physical field (i.e. the country in which they work), Skype enabled me to be in their 'virtual field', which, considering the content of this research, was even more important.

Negotiating access for Skype-interviews

Of course, using Skype came with some limitations as well. With regard to negotiating access, it was possibly easier for a potential interviewee to discard an online interview-request than a traditional one. It was therefore important to build trust, for which various strategies were used. Firstly, after approaching and interviewing gatekeepers (e.g. security units of NGO fora), snowball sampling was used. Snowball sampling is a sampling method 'whereby each person interviewed may be asked to suggest additional people for interviewing' (Babbie, 2010: 193). The risk of being forwarded to people of questionable value to my research was tackled by strictly testing whether the potential interviewee did fit in the originally proposed sample. Snowball sampling can build up trust since an interviewee knows that a friend or acquaintance of him or her trusted the interviewer enough to suggest the interviewee. This builds 'relational trust', which is an emotionally based form of trust, rooted in the fact that the interviewer and the interviewee have a mutual acquaintance or trustee (Norman, 2009).

In order to also win the 'rational trust' of participants, certain measures had to be taken (Ibid.). For instance, five interviewees (from various agencies and backgrounds) wanted to remain anonymous, while many others preferred a reference to their title rather than their name and organization (see Appendix I). Moreover, two interviewees asked for the transcripts to be locked and the recordings to be removed after the research would be finished, while one interviewee preferred not to be recorded at all. Lastly, several participants asked for the right to review the referenced paragraphs in order to prevent the possibility of linking back sensitive information to their organization. In an attempt to build this rational trust, strict compliance with these requests was important.

Challenges to the use of Skype for data-gathering

Donini and Maxwell (2013: 4) criticize the international aid worker's absence from the field by saying that it is the '“face-to-screen” relationship that increases the geographical, social, and emotional distance between the international (or capital-based senior national) aid worker and at-risk individuals and communities on the ground'. Although they may be right in this, the use of Skype in this research can hardly be seen as leading to an increased distance between the interviewer and the interviewees. Rather, this method of communication decreased the distance (in the virtual field) because of the interviewer's adjustment to the interviewee's normal way of work-related communication. A related critique is that Skype-interviews are less insightful since this research method prevents the build-up of a relation between the interviewee and the interviewer. However, the interviews were always preceded by the exchange of e-mails, while many interviewees were also contacted later on to ask for additional information, for feedback or for the approval of references. In combination with the earlier listed trust-building measures, this continued communication over an extended period of time guaranteed open and fruitful conversations.

The virtual field also comes with some technical challenges (i.e. virtual access barriers). Skype, for instance, requires high-speed internet and, even then, there is a possibility of interruptions due to a failing internet connection (Janghorban et al., 2014; Sullivan, 2012). As a consequence of the unstable internet connection in some of these conflict settings, interruptions indeed occurred occasionally, but, as experienced Skype-users, the interviewees were not distracted or taken aback by this. A more serious concern is Skype's right to share online acquired data with third parties (Sullivan, 2012). On the other hand, recordings, notes and transcriptions can always get confiscated in the field or stolen from computers, so this risk is not unique for Skype-interviews.

The absence of being in the physical field, however, did prevent other ethnographic research methods, such as observational data collection. Observational research modes might have something to add to how security officials perceive security management, technologies and Remote Management, but since they are operating in the 'virtual field' rather than the traditional, physical field, I expected the added value of traditional observational research to be marginal at best. Unfortunately, observational research in the 'virtual field' proved to have little to offer at this stage since security-related information is highly sensitive and many interviewees therefore either do not have social media accounts or use it for strictly personal updates.

A note on the interviewer

It is important to acknowledge that the interviewer unintentionally affected the answers of interviewees. The interviewer cannot be assumed to have been seen as objective and neutral. Barakat and Ellis (1996), for instance, report that self-presentation may bias the collected data. Personal characteristics, such as appearance and communication, are therefore relevant factors in interviews. Being a young, Western student with no work or living experience in a conflict setting and with little background in security, it is possible that I, at times, was seen as naive and ignorant. During my interviews, I used formal talk and referred to established concepts and examples to reduce this perception somewhat. Nevertheless, this perception also led to situations in which interviewees did not seem to perceive me as threatening, which may have made them more willing to share their thoughts and ideas with me.

Although I consider myself fluent in English and the international staff members were in general fluent as well, English was not the mother tongue of most of my interviewees, nor of myself. My questions were therefore not always flawless while my interviewees faced occasional difficulties with expressing themselves as well. Serious language barriers or failing interviews due to language issues did not occur.

Data analysis

Next to using Skype, I used iFree Skype Recorder, a free software that records Skype audio fragments, to transcribe the interviews. Together with the notes taken during the interviews on non-spoken information, the transcripts were uploaded in Atlas.ti. In Atlas.ti, the transcripts were coded and analyzed. The initial codes were based on a first reading of the texts but were adjusted and refined when the analysis progressed (see Appendix III).

Even though I was able to build up trust with the interviewees and they were willing to share confidential information (sometimes anonymously or off the record), there was some information in between the spoken lines as well. Fuji (2009) argues that there are multiple ways to derive information from an interview other than from the spoken words. Meta-data, as Fuji calls it, includes, amongst others, silences and evasions of questions. The fact that interviewees took a while before answering some questions or gave brief responses to a couple of questions hinted at the sensitivity of these topics and guided my approach to these issues in subsequent interviews.

Code of conduct

While doing my research, albeit not in the physical field, there were certain ethical guidelines that I observed. Based on the Wageningen University guidelines, as laid down in *Fieldwork in Hazardous Areas* (Hilhorst and Jansen, 2005), I have, first of all, always respected the dignity of my interviewees by being honest about my motivations for interviewing them and about the content of my research (although this has shifted somewhat over time). Moreover, all interviewees were asked for permission to record the interviews and for their preferred way of referencing to the interview. If any information acquired during the interviews could potentially harm the interviewees' position or the operations of an organization, I decided to not use this information. The recordings and transcribed interviews were handled with caution (e.g. locked) to prevent them from being leaked to third parties. Moreover, several interviewees were asked to approve of the references to their interview and propose corrections or additional information in order to assure a correct representation of their views.

In order to respect the principles of social science, the interviews were conducted for the sole purpose of gathering data and doing scientific research. Moreover, the research was, first and foremost, conducted in order to acquire the title of Master of Science. In case the research results would be disseminated to a wider circle than the supervisor, referent and interviewees, the participants in the research have been promised to be asked for permission and may propose a change of references.

Security managers and country directors are busy individuals who are tasked with serious responsibilities. Conducting interviews with them meant that they were temporarily distracted from doing the job they are hired to do. Interviews were therefore only undertaken if they were considered useful for this research. In addition, I tried to be as flexible as possible so that interviewees could, at all times, first fulfill their more important duties. In addition, this research aimed to not only 'prevent harm-doing' but also wished 'to do good' by disseminating the results among participants and by highlighting some best practices in different parts of the research.

Conclusion

The research question of this project is: How do technological developments affect the aid sector's security management as well as its view on and implementation of Remote Management? To answer this question, this research sets out to study 1) aid agency risk perceptions and their relation to security management, 2) the effects of technologies on security management and Remote Management, and 3) the views and implementations of Remote Management by aid agencies. In order to fill a gap in the literature, this research takes a 'middle ground' approach, which means that the goal of this research is to combine proximate and deep insights on aid agencies' risk management. The benefit of this approach is that it allows for general deductions and explanations, while still being able to relate these explanations to empirical findings. The data for this research was gathered from the scientific and the grey literature as well as from 31 interviews with security managers and country directors of the ICRC, NGOs and the UN in five conflict settings (Afghanistan, Iraq, Somalia, South Sudan and Syria). Lastly, the usage of Skype for the data collection fitted the technology-focused content of the research well and was therefore employed as a means of communication for most of the interviews.

Chapter 2: Theoretical framework

Concepts

Hilhorst and Jansen (2010) view humanitarian action as an activity that takes place in an arena in which various actors interact and negotiate aid delivery. Aid agency security management can, similarly, be seen as being formulated and negotiated in a 'security arena'. In this security arena, various actors (including donors, headquarters and threat sources) interpret, make sense of and influence the security management of aid agencies in diverse ways. It is important to emphasize that the very people who are subject to the security strategies (i.e. aid agency staff) are active 'negotiators' in this security arena as well. On the basis of the varying perceptions of the security environment, every actor will choose and use its own strategy to pursue its own interests. For instance, threat actors may issue warnings or commit attacks, while field staff may withhold or share security information in order to influence an aid agency's security strategies. Likewise, the way actors speak and write about the security environment (i.e. their discourse) further influences the security responses adopted by an agency's senior management. Foucault (2015) argued that discourses are weapons of power, control and fundamental confrontations, from which it can be deduced that discourses in the security arena intrinsically represent and aim to further the interests of the actors expressing the views or ideas. Thus, in this arena, views on risk perceptions and security strategies as well as explanations for insecurities are continuously negotiated, debated, managed, challenged and adjusted.

Thus, views and concepts in the security arena are always subject to debate and change. Nevertheless, it is worthwhile providing definitions of the main concepts of this research (i.e. risk perception, security, technological developments and Remote Management) in order to delineate the scope of this research and highlight its underlying assumptions. After defining these concepts, several theories on the underlying processes in the aid sector are discussed in order to be able to interpret and contextualize the empirical findings of this research.

Risk perception

In daily use, the term 'risk' refers to the possibility or probability of a negative consequence. It can also refer to a thing, person or group that poses a threat leading to the possibility of a negative consequence. Beck (1992: 19) argues that risks are systematically produced by modernization processes, specifically through techno-scientific developments and its indirect effects. In our society, risks are of a global nature but the chance of a risk turning into a catastrophe depends on someone's social risk position. Since the weak and poor have a worse social risk position, Beck (1992: 41) speaks of an attraction between poverty and risks.

Risks, however, are not neutral or objective. Rather, a risk is 'something non-existent, invented, fictive as the 'cause' of current experience and action' (Beck, 1992: 34). Thomas (1928: 572) wrote that a man's 'immediate behavior is closely related to his definition of the situation'. This led him to the definition of the famous Thomas Theorem: 'If men define situations as real, they are real in their consequences' (Ibid.: 572). Following the Thomas Theorem, Beck (1992: 55) sees risks as risks 'in knowledge', meaning that the perception of a risk and the risk itself are the same.

Taking as a starting point that the risk perception and the risk itself are the same, this research uses a constructivist approach. This means that reality is understood 'in the form of multiple, intangible mental constructions, socially and experientially based, local and specific in nature (...) and dependent for their form and content on the individual person or groups holding the constructions' (Guba and Lincoln, 1994: 110-111). Objective risk analyses are impossible, so the security manager's risk analyses and views on security risks are perceptions and interpretations of the material world.

Since security risk perceptions are socially constructed and based on social interactions and subjective experiences, these perceptions can only be understood in relation to their physical, organizational and social environment (see Ibid.). Thus, aid agency risk perceptions are inherently negotiated by a plethora of actors, including staff members, headquarters, armed groups, local authorities and beneficiaries. All of these groups affect the risk perceptions of an aid agency's security manager through their actions and language. Their influence can be open and intentional as well as veiled and unintentional. The security manager, by formulating situation reports, providing briefings and writing Standard Operating Procedures, aims to manage the risk perception through formulating an agency-wide perception of the risks in a country. Irrespective of the credibility of the security manager as a security expert and as a senior staff member, this centralized and managed risk perception is likely to be contested. For instance, many national staff members claim that their international counterparts overestimate the risks (Egeland et al., 2011), while armed groups may renew threats in order to direct the policies of an aid agency. In brief, risk perceptions can never be completely managed and will always be subject to contestation and negotiation in the social interface of a security manager and his or her environment.

Nevertheless, the senior management's perception of a security risk informs the response to this risk (i.e. security management). Security management can be defined as '[t]he attempt to reduce exposure to the most serious risks [...] by identifying, monitoring and tackling key risk factors' (Egeland et al., 2011: xv). Security management can take various shapes, varying from accepting the risk or defending the object at risk to mitigating it or avoiding it altogether. Just like the perception of the risks, the decisions on security strategies are openly, veiled, intentionally and unintentionally negotiated and contested by a variety of actors.

The recent increase in attention for security management has led to a debate on how aid agencies respond to risks. Beck (1992) argued that modern societies are increasingly occupied with managing risks. In his footsteps, critics argue that aid agencies have grown risk averse which affects their aid delivery. For instance, expatriate staff often hides in well-protected compounds, a process which Duffield (2012) calls 'bunkerization'. Collinson and Duffield (2013) even argue that humanitarian agencies used to worry about the risks that beneficiaries faced (e.g. starvation and displacement), but are now mostly concerned with (security) risks to themselves. On the other hand, it can be argued that aid agencies simply respond to the rising numbers of reported incidents by professionalizing their security management. In this vein, risk aversion and risk awareness are two sides of the same coin.

Security

The definition of security is usually assumed rather than provided in the existing literature. Admittedly, there are a few complicating factors in defining security. Firstly, the concept is used in a broad array of fields, varying from banking (e.g. investment security) and computing (e.g. data security) to physical protection (e.g. by army and police). Secondly, especially after the attacks of 9/11, there seems to be an inflation of the word 'threat' (defined as: a danger in the operating environment' (HPN, 2010: xix)). This inflation has led to an excessive use of the word 'security', which hollowed out the term by exploiting it to justify a wide range of unrelated measures (e.g. against climate change, lone wolfs, immigration, terrorism and cybercrime).

In fact, only one humanitarian report attempted to shed some light on the term 'security' by defining it as the: '[f]reedom from risk or harm resulting from violence or other intentional acts' (HPN, 2010: xviii). One of the strengths of this definition is that it includes both the absence of harm and the absence of potential harm (i.e. risk). It also refers to the *'freedom* from risk or harm', which means that security entails a complete absence of any potential harm. Although this is unlikely to be achieved in a conflict setting (since it is impossible to mitigate all risks completely), the definition should be seen as an ideal-type of security and is therefore conceptually useful. Thirdly, the definition only includes human-made risks and harm in order to prevent an inflation of the term security by confusing or conflating it with the term safety (which, then, refers to risks or harm from non-human threat sources).

Nevertheless, there is also a questionable aspect to this definition, especially when it is used for studying aid worker security issues. This definition suggests that security only refers to a situation without intentional acts of harm-doing. However, in many conflict areas, aid agencies are victimized accidentally as well. As a matter of fact, the report itself even discusses this risk of collateral damage. The security management of aid agencies does indeed go beyond the mere protection against targeted actions. Therefore, this research will use the following, slightly altered, definition of security: 'The freedom from risk and harm resulting from violence and other acts'.

Technological developments

Technology (in daily use defined as: the use of (scientific) knowledge for practical ends) is a central process in modern societies. According to Beck, technological progress is the centre-piece of modernization, affecting the social relations, societal characteristics and cultural values (Beck, 1992: 50). While other scholars on modern societies may focus more on other aspects of modernization, such as rapid change, new societal orders and economic progress (e.g. Bauman, 2004), these aspects are enabled or reinforced by technological progress. The development of technologies is not limited to the era of modernization. Even the use of stone for axes and the invention of the plough are (ancient) examples of technological innovation. The technological innovation in our age, however, is unique because of its unprecedented speed (Beck, 1992).

The conceptual delineation of 'technological developments' is naturally somewhat artificial due to various reasons. Firstly, the development of a technology is always a long-term process and every technology has its roots in earlier technological developments. Secondly, some technologies may date back quite a while but their commercial use can be quite recent (e.g. internet). Lastly, some technologies may have been around and used commercially for a longer period of time, but its implementation by the aid sector can be more recent (e.g. GPS). The reason to still include these technologies in this research is that this research is concerned with the effects of technologies on the aid sector and these effects can only be studied once these technologies are implemented.

In short, this research includes technologies that have been discovered and implemented by aid agencies in recent times. It includes a wide range of technological tools, including communication technologies (e.g. social media, Skype, text messaging), information-gathering technologies (e.g. GPS, drones, satellites), information-analysis technologies (e.g. databases, Big Data, mapping tools) and distribution technologies (e.g. cash transfers).

Remote Management

There is a multitude of definitions and interpretations of Remote Management in the literature. Stoddard et al. (2010: 7), for instance, define Remote Management as 'an operational response to insecurity, [which] involves withdrawing or drastically reducing international and sometimes national personnel from the field, transferring greater programme responsibility to local staff or local partner organisations, and overseeing activities from a different location'. Carle and Chkam (2006) emphasize the necessity of the decision and its consequences by defining Remote Management as 'a reactive position where, by necessity, international staff are remote from national staff and, by necessity, there is a transfer of decision-making and skills to national staff, and capacity-building of national staff in order to get the originally proposed job done'. Steets et al. (2012) propose a scale, arguing that the further a threat deviates a program from the ideal of full, safe access, the more remote the program becomes.

On the basis of the literature (see: Carle and Chkam, 2006; Donini and Maxwell, 2013; Egeland et al., 2011; Steets et al., 2012; Stoddard et al., 2010), Remote Management will be defined in this research as: 'a mode of operation in which international staff, either after relocation, after evacuation or by design, manages a project from a distant location because of high or increasing security risks, while national staff members or local partners implement the project on the ground'.

Since this definition is different from existing definitions, it is worthwhile discussing this definition in some detail. There are two main points of attention. Firstly, this definition of Remote Management includes projects that are implemented through national staff as well as projects that are implemented through local partners. Although Stoddard et al. (2010) include both options as well, other definitions may exclude projects implemented by local partners (see e.g. Carle and Chkam, 2006). However, since these projects are often managed and overseen by international staff, located in a safe, distant place due to security concerns, this definition does include projects implemented by local partners as Remote Management projects.

Secondly, the definitions provided in the literature do not include projects in which international staff is managing projects from a distance *by design,* as a response to the volatility of the context. By emphasizing the reactionary element of withdrawing staff from the field, projects that are remotely managed after due planning are neglected, even though the use of Remote Management in countries like Afghanistan and Somalia has become so common that it can hardly be labeled as 'reactive'.

Social science theories on the aid sector

In order to bridge the gap between proximate and deep explanations of aid agencies' security approaches, social science theories are employed to explain the results of the collected empirical data. In this chapter, these theories are briefly introduced. The interpretation and application of these theories will be discussed under separate headers in the empirical chapters. These theories are not used as a framework in which the empirical findings are incorporated since this would most likely result in an abstract, theoretical research on the deep causes, in which incidental evidence would be used to back the theoretical claims. Rather, as part of the 'middle ground' approach, these theories are used to explain and analyze the results of the collected empirical data on the relations between security management, technologies and Remote Management.

Since these theories usually rest on views rather than facts (e.g. they almost never refer to the realities in the field) and since they rarely take the role of technologies and Remote Management as a central factor, this research contributes (and criticizes) these theories. By trying to bring together the practices of aid agencies on the ground and the fundamental effects of technologies and Remote Management on aid delivery as well as by theoretically explaining the collected empirical data, this research aims to use the 'middle ground' approach and, thus, tries to fill a gap in the literature.

A Foucauldian view

The writings of Foucault offer the first critical perspective on the role of aid agencies. With regard to power, Foucault (2003) recognized that its essence had changed dramatically in the nineteenth century. Earlier, sovereigns had the right 'to take life or let live', which came with disciplinary measures of surveillance, training and punishment of individual bodies. In the new era, sovereigns also got hold of the power to 'make live and let die', meaning that subjects only could live by the grace of the sovereign. This mode of power required regulatory technology to control the man-as-species (unifying individuals in a global mass) (Ibid.: 240-243). This 'massifying' mode of power (i.e. power focusing on the mass rather than the individual) resulted in 'a "biopolitics" of the human race' (Ibid.: 244-249). This biopolitical power is, nowadays, also wielded by aid agencies that control and regulate large groups of beneficiaries (e.g. refugee camps).

Biopower, the power of biopolitics, is scientifically based and can, through general decisions, make people live or let them die, in order to protect the population as a whole against 'internal dangers' (Ibid.: 249). Biopower deals with elements in the population in such a way as 'to optimize a state of life' and requires a comprehensive system of 'coordination and centralization' (Ibid.: 246, 250). The norm (as a prescriptive standard for living) is applied to both the individual bodies (as the old power) and the general masses (as the new power). Norms, through technologies of discipline and regulation, aim to steer bodies and populations alike, since the norm of discipline and the norm of regulation meet in 'the normalizing society' (i.e. society that aims to adjust human and mass behavior in order to make them comply with the societal norm) (Ibid.: 252-253). A contemporary example of this are aid agencies' advertisements in refugee camps encouraging Western views and ideas.

Noteworthy, Foucault introduced the 'boomerang effect' of colonial practices, which referred to the tendency of colonizing powers to bring the methods used in the colonies back to the colonizing countries (Foucault, 2003: 103). Many 'apparatuses, institutions and techniques of power' were in this way applied to Western populations as a consequence of colonial experiences. Foucault called the consequences of this boomerang effect 'internal colonialism' (Ibid.). For this research, it means that aid agencies' activities may very well be copied in or exported to the West.

Beck's critique

According to Beck, techno-scientific developments are the major source of risks in modern societies. Beck (1992: 19) claims that modern societies aim to systematically tackle modernization-induced risks by using a rational, scientific response, which he labeled as the 'risk society'. In order to detect and estimate risks, rational scientific probability statements and calculations are employed, even though this ignores the fact that science itself is based on assumptions, realities and values (Ibid.).

In modern societies, the aim is to rationally prevent, minimize and channel risks as much as possible in order to allow the modernization processes to continue without the risks exceeding the limits of what is seen as tolerable (Ibid.: 19). Therefore, modern society's utopia is defensive and focuses on prevention and, especially, precaution (Ibid.: 69; Beck, 2006: 334-335). Aid agencies, as part of modern society, have been implementing a range of technologies in order to prevent security risks from materializing, but this has led to new worries about the risks of failing technologies. Therefore, just like the modern societies in which they originate, the aid sector 'is increasingly occupied with debating, preventing and managing risks *that it itself has 'produced'* (Beck, 2006: 332)[1].

The question arises why aid agencies are still operating in dangerous conflict settings if they have grown risk averse. This may be explained by the idea that aid agencies have a risk-reducing factor as well. Without their work, millions of people would live in such abject poverty that they might become a risk to Western modernization (e.g. by massively migrating to the West or by resorting to violence). As beacons of Western modernization, aid agencies reduce these risks to the West at the cost of posing risks to themselves by operating in these areas. At the same time, in order to mitigate and manage the risks in their direct environment, aid agencies have aimed to increase their resilience by emphasizing security efforts and methods that can help them to 'stay and deliver' (see Egeland et al., 2011). Question as to whether the world is indeed becoming more dangerous for aid workers and these resilience-enhancing efforts are needed in the first place, however, are rarely put and hardly considered (for an exception, see Dandoy and Pérouse de Montclos, 2013).

According to some, Beck's 'modern' view on risks can be replaced by a 'post-modern' perspective. Duffield (2012), for instance, states that the current emphasis on resilience is symbolic for the shift to a postmodern notion of risk that internalizes risks in society. In this view, aid agencies are required to be open to risks as they inevitably come with chances to renew and improve the organization and reality. Aid agencies, therefore, are no longer supposed to avoid risks. Instead, they need to try to manage (and make use of) them by being prepared and being adaptable (Ibid.). While Beck's definition of resilience focuses on the reduction of the risks that are introduced with every new technology, Duffield (2012) sees resilience as the tendency of Western, neo-liberal societies to be open to risks and use them to further their goals. Duffield's views are worthwhile mentioning as a critique of Beck's ideas. However, they have by no means replaced Beck's theory on risks, which is still widely used and highly valued in scientific circles. Thus, Beck's work will also be used in this research for analyzing the empirical findings.

[1] Italics are mine

Politicization of aid

A very prominent explanation in the scientific literature for the presence of aid workers in dangerous areas is the perceived political interests of the West in reducing the (potential) threat caused by these regions. Duffield (2001), for instance, argues that aid agencies are part of a global liberal governance that aims to 'securitize' international assistance (i.e. transform the nature of aid in order to make it a means for improving the security of Western states). The political nature of the goals that the aid sector pursues, has gained significant attention in the aftermath of the terrorist attacks on the World Trade Centre in New York, in 2001. Colin Powell (2001), then US Secretary of State, voiced this development most notoriously by telling an audience of NGO representatives that NGOs are 'a force multiplier for us, such an important part of our combat team'. Later on, he referred to the 'use of foreign aid' as part of the 'front line of US defense' (Ibid.). In addition, in the years after the 9/11 attacks, NGOs that were unwilling to participate in the War on Terror were heavily criticized and bullied by officials in and near government circles (Stoddard, 2003b).

One trend worthwhile mentioning with regard to the politicization of aid is the rise in 'integrated missions', in which the UN's peacekeeping missions (with its political and military aims) and aid agencies' humanitarian activities are integrated (Donini and Maxwell, 2013). In some cases, however, this has led to the subordination of humanitarian goals (from NGOs but also from humanitarian UN agencies) to the global community's political and security aims (Donini and Minear, 2006: 17). This has resulted in a concern that the joined approach might raise the risk for aid agencies of being targeted for political reasons (Ibid.), although this statement is questioned (Stoddard et al., 2006).

There are also critiques and comments on the view that aid is becoming more and more politicized. Some authors, for instance, argue that there is no trend of politicization since aid was a political tool during the Cold War as well (Dandoy and Pérouse de Montclos, 2013), while others claim that it is hard to find factual evidence for the link between aid and Western, political goals (Fast, 2010). In addition, some humanitarian reports argue that it is not just the politicization of aid, but also (or rather) the fact that aid is intrinsically Western or has a Western nature that leads to violent incidents against aid agencies (Egeland et al., 2011; Stoddard et al., 2009; Stoddard and Harmer, 2010). Although these remarks are helpful and relevant, the basic view on aid as politicized or politicizing still holds.

Militarization of aid

The militarization of aid goes one step beyond the politicization of aid for security reasons. Whereas the politicization of aid refers to aid agencies aiming to improve global security by selective aid provision, the militarization of aid refers to the increasing convergence and overlap of aid and the military. Militarization of aid can be translated into practice in various ways. Firstly, in a 'top-down' approach, aid provision can be embedded in one of the parties to the conflict (Pérouse de Montclos, 2014). Secondly, taking a 'bottom-up' perspective, aid workers can use force to protect themselves or demand the use of force for protection purposes (Ibid.).

The first type of militarization, as aid provision being embedded in a party to the conflict, is often mentioned as a reason for concern, because it blurs the distinction between 'neutral, impartial and independent' aid agencies and belligerents. While aid agencies often align with one of the sides in a conflict (e.g. against Al Shabaab or alongside UN peacekeepers), another example of this type of militarization is the provision of relief packages by national militaries (Duffield, 1997), such as quick impact projects to win 'hearts and minds' (Collinson and Duffield, 2013). Similarly, in the early 1900s, the Red Cross used to be embedded in the national armies of, for instance, France and the US (Dandoy and Montclos, 2013), while aid packages to Afghanistan and Nicaragua in the 1980s were also militarily motivated (Pérouse de Montclos, 2014). Although far from new, top-down militarization of aid is still cause for concern.

The second type of militarization, as the use of force to protect aid workers or recipients, is nowadays exemplified by the integrated approaches (in which the aid agencies deliver whilst being protected by UN peacekeepers), by aid agencies' usage of armed protection (e.g. Interview 9 & 11) and by the Responsibility to Protect (R2P) discourse (e.g. Donini and Maxwell, 2013; Pérouse de Montclos, 2014). Again, however, this type of militarization is not new. For instance, in the twelfth Century, military force was used by the Order of Saint John of Jerusalem (which started off as a charity), whilst liberation movements in the 1970s likewise mixed up aid and military force (Pérouse de Montclos, 2014). Although the militarization of aid may not be a new phenomenon, its implications still pose some serious challenges for the aid agencies of today.

Remoteness and virtual reality

One of the main disadvantages of Remote Management and the bunkerization of aid is the increased expatriate staff 'remoteness' from the field. Next to an increased geographical distance, the remoteness from the field leads to an increased social and emotional distance from the field among international staff as well, according to Donini and Maxwell (2013). The 'face-to-screen' relationship, which has come to replace 'face-to-face' contact, renders humanitarian aid an activity of remoteness instead of proximity and makes it even more top-down than it historically already was (Ibid.). The effects of this detachment of the field are believed to cause, for instance, a perceived (but unjustified) increasing danger for (international) aid workers in the field (Duffield, 2012) and lower quality aid due to an ignorance of the social, political and economic realities in the field (Collinson and Duffield, 2013).

A final worrying consequence of the increased remoteness is the changing emotional and psychological relation of internationals to the field. The 'cyber-humanitarianism' of our age transforms aid provision into an online rather than a physical reality (see Donini and Maxwell, 2013). Through its use of technologies, the increased remoteness builds in a mechanical distance, which transforms humanitarian aid into a 'virtual reality for global audiences' (Sandvik and Lohne, 2014: 12). This leads to a situation in which suffering is better visible, but likely to be met with reduced empathy.

Commercialization of aid

Due to aid agencies' increased distance (and detachment) from the field and the role that they increasingly play as global risk reducers by using their biopolitical power over populations that are potentially threatening to the West (or its modernization processes), the position of aid agencies in the global arena is subject to change as well, which has various consequences for the way aid agencies operate and portray themselves. In a critical view on aid, agencies are (company-like) actors which can be paid to deliver services that reduce the risks to the West and which compete over 'contracts' (i.e. grants). This is the image that some scholars draw when referring to the aid sector as the 'humanitarian enterprise' (e.g. Donini and Minear, 2006; Collinson and Duffield, 2013; Donini and Maxwell, 2013).

As aid agencies are becoming more business-like (e.g. through competition over grants and elaborate reputation management), there is progressively more governmental 'development aid' going to private companies as well. Another factor that blurs the distinctions between aid and business is the rapid rise in the number of partnerships between aid actors and the (traditional) business sector (e.g. the UN's partnership with Vodafone (UN, 2008)). The other way around, companies have begun to take an interest in humanitarian activities, mostly for branding purposes or, as Žižek (2009) claims, to give capitalist consumerism a moral component and buy off the consumer's guilt while supporting the cultural aspects of the capitalist system (i.e. cultural capitalism). In short, the aid sector is faced with blurring lines between aid and business activities, which results in a commercialization of aid.

Conclusion

In the security arena, a variety of actors negotiate, manage and challenge the risk perceptions and risk management strategies of aid agencies. The main concepts of this research (i.e. 'risk perception', 'security', 'technologies' and 'Remote Management') are inherently socially constructed and negotiated. As such, they are primary examples of the open and veiled as well as intentional and unintentional powers that social actors, through their discourses and activities, try to wield over the definitions and perceptions of these concepts. Bridging the gap between proximate and deep explanations of aid agencies' security approaches, this research introduces several social science theories that will be used to explain and analyze the empirical findings in later chapters. From a Foucauldian point of view, aid agencies can be seen as actors wielding biopolitical power over beneficiaries. Next, Beck claims that Western societies are increasingly occupied with preventing risks. Also, a mainstream scholarly school argues that aid is more politicized than ever, while the militarization of aid poses another cause for concern. Furthermore, aid agency staff, through Remote Management, is progressively detached from the field. Lastly, there are signs of a conflation between aid and business, leading to a commercialization of aid.

Chapter 3: Technologies in the aid sector

Technologies in the aid sector

As a central process in modernization, the rise of technological developments affects the aid sector's activities significantly. At a progressively large scale, aid agencies adopt and adjust existing military and commercial innovations for humanitarian purposes. For instance, Unmanned Airborne Vehicles (UAVs) have a military history but are lately deployed by humanitarians after big natural disasters for needs assessments and mapping purposes (Interview 29). Likewise, electronic devices were first designed for the exchange of private information but have recently been used by aid agencies to collect data from the field, including information on the needs of recipients and on the conflict dynamics (Mayo, 2014; Interview 16).

The ICRC, NGOs and the UN are all using technologies, but there seems to be virtually no formal framework for the implementation of technologies on the institutional or organizational levels of aid agencies. Hypothetically, smaller agencies could be expected to be more agile, while bigger agencies face some sort of 'big tanker syndrome' (i.e. they are slow to turn around and innovate) (Interview 29). On the other hand, bigger agencies usually have a larger share of private funding, which means that they have more liberty to research new tools and develop existing technologies, whereas reliance on institutional funding reduces the liberty to innovate (Ibid.). The jury is therefore still out on which type of aid agency is most innovative or best able to use technological tools in its activities.

Many security managers and country directors of aid agencies seem to be unaware of their reliance on technological innovations. The widespread use of commercialized technologies, such as social media, electronic cash and satellite-based maps, undermines the recognition of the effects of these technological advances on aid delivery. However, the profound implications of technological progress on the aid industry is recognized by the aid sector at large, be it by the Red Cross (IFRC, 2013), the UN (UNOCHA, 2013) or NGOs (EISF, 2014). Although incorporation of technologies in daily work of aid agencies is slow and comes with periodic setbacks (Interview 31), its rise is unstoppable.

Reasons for using technologies for aid delivery in conflict settings

Efficiency

The most obvious advantage of continuous technological progress (i.e. the 'digital transformation change' (Interview 29)), is the efficiency with which activities can be undertaken. For instance, the use of information and communication technologies (ICTs) by aid agencies has sped up their ability to respond in fast changing (conflict) environments. Exemplary for this is the use of simple Short Message Service (SMS) alert systems, which allow a designated person to inform groups of people at the click of a button (Interview 25). Also, the almost universal coverage of satellites has reduced the need of users to find a place with internet, cell phone or GPS signal reception (Interview 29). This enables aid workers to always keep in touch with each other and communicate relevant information at any given time.

Information technologies are reducing the time delay between assessments and response as well. When a disaster strikes, aid agencies can now make use of advanced mapping platforms to design a quick and efficient response while drones and satellite imagery (e.g. UNOSAT) can be used to give a detailed, safe and (relatively) cheap image of the damage caused (Interviews 27 & 29). Rapid assessments are therefore faster than ever. In addition, social media and mobile phones can be employed by beneficiaries to approach aid agencies with requests for aid, which reduces the time delay of aid delivery even further (IFRC, 2013: 48-49; UNOCHA, 2013). Although social media can be an overwhelming source of information at first, improved Big Data software and the use of Artificial Intelligence make it an ever more useful tool for acquiring information (Meier, 2015a).

Aid agencies are increasingly using (or discussing the possibility of using) electronic devices for collecting data of beneficiaries (Interview 1, 16 & 29). These devices are usually taken by a team into the field for surveys with recipient communities. Electronic questionnaires are set-up and filled in by the teams when visiting the target group. Upon completing the survey or when connected to the internet, the collected data is uploaded into a database which can be used for assessing needs and designing projects (Interview 16, 29 & 31). This digital data collection has a lower fault margin than manual data collection and the information can be analyzed much faster (Interview 29). Thus, just like improved communication and information tools, advanced data collection and analysis have a profound effect on the efficiency of aid agencies.

Effectiveness

Thanks to the development of new technologies, the effectiveness of aid delivery has been vastly improved as well. In the field of early warning, food prices can be monitored on mobile phones so that potentials victim can be warned and assisted in time (IFRC, 2013). On a more advanced level, satellites and advanced computer models can estimate the risks of natural events, such as droughts and food shortages (Ibid.: 104-110). In addition, oceanographic radars can predict tsunamis (Ibid.), big data analysis software can be used to reduce the response time by detecting trends and risks such as outbreaks of diseases (UNOCHA, 2013), and detailed maps provide all the necessary information for humanitarians when they are planning their projects (see Humanitarian OpenStreetMap Team, 2015). The availability of better knowledge and research informs the preparedness of aid agencies and improves their effectiveness as a consequence.

Secondly, there is a wide array of implementation possibilities related to technological progress. The discovery of new medicines and new water filters, for instance, have greatly improved the health of many individuals. The rise of electronic cash is noteworthy as well (Interview 29). While the delivery of physical cash is often limited due to logistical and security constraints, the use of mobile cash is a progressively popular solution (Interview 29 & 31). Another tool improving the effectiveness of the implementation of aid projects is electronic registration, which helps aid agencies to determine which beneficiary is entitled to which goods and what has been handed out already (Interview 29).

Thirdly, the advances in technologies have contributed to better harmonization of the plans of aid agencies. Although the work of OCHA, tasked with the coordination of humanitarian activities, does not always meet the expectations (Interview 19 & 28), improved communication exchange and information management allow for better coordination and more effective aid delivery (UNOCHA, 2015). Similarly, the main role of NGO fora, the sharing of (security) information, significantly benefits from the availability of information and communications technologies (Interview 21). As long as the risk of an information overload is avoided, this information leads to better preparation, implementation and collaboration, and, thus, to more effective aid delivery.

Visualization

Due to the development of technologies, information can be more easily visualized and transferred. This can be relevant for various purposes. UNOCHA, for instance, is a frontrunner in the creation of visually attractive infographics in order to convince UN member states to fund its activities[2]. Likewise, Medair found that using drones for information collection can also produce images that are valuable for fund-raising purposes (Interview 29).

In addition, the use of maps has proven to be extremely useful for giving a fast and simple visual overview of a crisis situation. When, after the elections in 2007, unrest broke out in Kenya, Ushahidi[3] created a map showing the incidents that were reported by witnesses in the field via the web-form, e-mails or SMS text messages, often just moments after they had occurred in the field (Meier, 2011). The combination of the speed of the data collection and the clear way of displaying the information made it a highly valuable tool (Interview 28). In addition, Geographic Information System (GIS)

[2] Personal communication, UN official
[3] Ushahidi (meaning 'testimony' in Swahili) is a free, open-source data mapping platform.

technology can add spatial, demographic and other information to these maps and thereby visualize the vulnerability of populations (IFRC, 2013: 85-87).

The overload of information makes it more and more important that data can convey a message as intended. Graphs, infographics, maps, videos and drone images are able to present the collected data fast, clear and visually attractive (Interview 29). In brief, visual outputs may be useful for aid agencies when they account for their activities or pledge for funds, while they can also help to make aid delivery even more efficient and effective by displaying information clearer and quicker (Ibid.).

Democratization

The continuing rise in access to technologies has beneficial consequences in terms of relative power positions as well. While refugees and remotely located individuals were easily neglected, the almost universal coverage of mobile phone satellites and the enormous rise in mobile phone ownership have made it possible for almost every individual to speak out (and ask for assistance) (UNOCHA, 2013: 19). Also, when beneficiaries have complaints, they can call or text the aid agencies and share their concerns or discontent (Interview 2, 20 & 31), the success of which depends to a large extent on the agency's ability to make beneficiaries aware of the existence of the 'hotline' (FSAC, 2013). In addition, these mobile phones can be used for crowdsourcing (or crowdseeding) information in which the beneficiaries send needs or security updates to the aid agency in order to provide it with relevant field information (UNOCHA, 2013). Furthermore, to counter the reverse trend, the rise of technologies allows beneficiaries to gather more information about the aid agencies (EISF, 2013), which reduces the information (and power) imbalance between the two groups.

This imbalance is further reduced by the ability of new technologies to decrease the symbolic power gap between the aid agencies and their beneficiaries. Standing in line and 'begging' for food or other items can be humiliating. In response, Medair and other agencies began to use Last Mile Mobile Solutions, a software system that stores information collected in the field and digitally calculates the type and quantity of goods to be distributed (Kaiser and Fielding, 2014). The intended recipients receive personalized ID-cards and instead of 'waiting in line', they only come to pick their goods up, which restores their dignity (Interview 29). Mobile cash transfers have a similar effect by altogether abandoning the need to stand in line (Tafere et al., 2014).

Moreover, due to technological progress, it has become much easier for aid agencies to reach their own staff in the field. For example, although not being at a place where it can replace face-to-face trainings, aid agencies have begun to develop online learning platforms, in which local staff and local implementing partners can get security trainings (Interview 26). Also, national staff can be equipped with phones and receive SMS alerts (Interview 25), just like their international counterparts, democratizing the access to information within the aid agency. Thus, technologies lead to more democratization by giving beneficiaries a voice, by decreasing symbolic power inequalities and by reducing information imbalances between different staff members.

Critique and challenges to the use of technologies for aid in conflict settings

Opposition against technological developments

A variety of actors oppose the use of technological tools for humanitarian aid in conflict areas and subsequently hinder their implementation. Firstly, the environment in which an agency operates may be hostile to technologies. Most notoriously, armed (terrorist) groups are opposing their use. For instance, Al Shabaab, in Somalia, is banning the use of technologies since they fear that GPS technologies and smart phones are used for espionage by Western countries (Interview 31). Likewise, the Taliban in Afghanistan is likely to target aid workers registering GPS coordinates or using smart phones, as they think that this information can be used by the government to attack them (Interview 1). By using these technologies, aid workers are also identifiable as working for a Western aid agency to which the Taliban and similar groups may oppose (Mayo, 2014: 47).

Also within aid agencies, there can be opposition against the use of technological tools. For example, aid agencies are aware of the military connotations that many technologies may have. Drones, in particular, suffer from the strong association with military activities which hinders its more widespread use (Interview 29). Similarly, voice- and iris-recognition devices, next to being hard to cross-check, are seen as drawing an unwanted link between the aid agency and the military (Interview 2). Moreover, the management of aid agencies may not see a strong need or be hesitant because initial costs are often high, while (implementing) staff tends to argue that they do not have enough time for testing or getting used to new technologies (Interview 29). Local staff may also fear that using technologies will create the image that they are wealthy, which makes them a target for criminals (Interview 12; Mayo, 2014)

Donini and Maxwell (2013: 385-386) claim that distancing technologies have a negative effect on the relationship between aid workers and beneficiaries. They argue that the reliance on technologies 'increases the geographical, social and emotional distance' if 'face-to-screen' relationships replace face-to-face relations (Ibid.: 386). In a similar vein, the IFRC (2013: 137-138) writes that technologies reducing face-to-face meetings create 'a real danger that institutional notions of accountability towards local populations will cease to take any form that is meaningful from their perspective'. Opposition against technologies therefore does not only come from threat sources in the field, but also from within the aid agency and from scientific circles.

Unmet conditions for implementing new technologies

The use of technologies often relies on supporting networks. Even a very simple cell phone needs to be charged and requires satellite coverage to be functional. As a consequence, the presence of reliable electricity and reliable internet connections is essential for many technologies (Interview 29). Although satellite coverage is almost universal and back-up systems are in place to cover potentially failing systems, actors may still try to prevent the use of technologies by undermining these supporting systems. For instance, in times of rising tensions, governments may jam the communication networks (Interview 27).

A second condition to be met before technologies can be used effectively is the presence of technical know-how among the intended users, both in terms of how the technology should be used and how it can be fixed if it is malfunctioning (Interview 12). Moreover, technologies can only be useful if there is an understanding about its goals and the processes it aims to improve. A calculator, for instance, has no use for someone without any knowledge on mathematics (Interview 29). It may therefore be necessary to train staff in order to provide them with more knowledge on the underlying processes as well as how technologies can assist them and can be fixed when they break down.

Inequality caused by technological innovations

Although technological innovations give more and more people a voice, there are still groups of individuals and populations without internet connection and mobile phones. Marginalized and vulnerable groups, in particular, are likely to lag behind in terms of access to technology, leaving them even more vulnerable and marginalized (IFRC, 2013: 30-31; UNOCHA, 2013: 35-37). As opposed to groups with technologies that can ask for assistance (e.g. through crowdsourcing), these groups will have 'to be found' by aid agencies, which harms their relative position in comparison with other beneficiary groups.

Moreover, there are political consequences for communities if actors that control the new, technologically advanced communication lines with the aid agency are not the traditional power holders. Aid agencies may namely be inclined to communicate with those that own or are willing to use these technologies, but this may have unwanted effects on the local power dynamics (see UNOCHA, 2013).

Within organizations, technologies might cause inequality as well. National and local staff members are much less likely to own or have access to communications tools than their international counterparts (Interview 21; Mayo, 2014: 47). When (the international staff of) an aid agency moves out, it often takes laptops and cell phones along. Part of the explanation is that national staff faces higher risks when carrying technologies since they are more likely to be seen as collaborating with a Western agency or as relatively wealthy (Mayo, 2014). However, aid agencies also assume that they do not need all these technologies since national staff members 'have their own networks' (Ibid.). Thus, the unequal access to technologies can create rifts between and within beneficiary groups as well as between the national and international staff of an aid agency.

Reliability of data

Social media can be a valuable and extremely fast source of information. However, sites as Twitter and Facebook are free and open-source networks which do not (necessarily) give a reliable image of reality. First and foremost, some groups, especially the socioeconomic upper-class, will be overrepresented in the data collection, whereas poorer groups in the society may share nothing or only very little online (UNOCHA, 2013: 35). Social media may therefore provide a very distorted picture of the needs and risks that an aid agency will come across in the field. The use of this big data as source of information should therefore be used very carefully when taking decisions (Ibid.: 34).

Moreover, the amount of online data is so large that it can easily result in an information overload, hiding the relevant information in its abundance. There is a related risk that a lot of time is spent on gathering information which reduces the attention given to the analysis of the data (Ibid.: 38). Lastly, information is increasingly processed and owned by private companies. These companies offer or host social media, communication networks and data analysis software. The fact that they have no humanitarian interests may be a cause for concern in assessing the reliability of the data that they offer (IFRC, 2003: 35). Technological tools do therefore not necessarily lead to more reliable data.

An unstoppable trend

Many of the above mentioned practical challenges to the use of technologies for aid in conflict settings are due to the infancy of these technologies. Initial opposition against newly developed technologies is commonplace. For instance, in the early days of mobile phones, people were worried about mobile phones impinging upon personal liberties and being harmful to the health of the user, while, nowadays, the use of mobile phones is broadly accepted (Interview 29). In addition, the fear of reduced accountability as a consequence of the use of technologies is understandable but remains, as of yet, speculative rather than well-researched. In terms of meeting preconditions, providing the required education and training is a rather easy requirement to meet (Interview 29), especially in a time in which technological tools are increasingly user-friendly. Moreover, the improvement and expansion of supporting networks is continuing as well (e.g. 4G mobile communications technology).

Inequality due to technologies can be reduced (or turned around towards more equality) by making technologies more easily accessible to marginalized populations. As an example, WFP distributed mobile phones to drought-affected populations in Kenya (IFRC, 2013). This has the added (democratizing) benefit that there is no or less need for a (powerful) gatekeeper or interlocutor. The reliability of data is a challenge that aid agencies face in any conflict setting, regardless of their use of technologies. The use of technologies for data collection does, however, not replace existing data collection methods but can be seen as complementary. Improved analysis software, moreover, makes online data increasingly reliable and relevant as a source of information (Meier, 2015a). Lastly, extensive reports outline the many ways in which aid agencies can protect themselves against the challenges and risks that result from the digital transformation change (e.g. EISF, 2010, 2014). In short, the practical challenges outlined above are worthwhile addressing but are not insurmountable. There are, however, also theoretical concerns about the influence of technologies on the nature and future of aid.

A Foucauldian view

From a Foucauldian perspective, technologies are an incredibly useful means for aid agencies' exercise of both (the old) disciplinary power and (the new) biopolitical power, since technologies can make surveillance and training of individuals as well as the regulation and control over the man-as-species much more efficient and effective. By using Big Data and tracking devices (which enable disciplinary power), every individual can (potentially) be traced and controlled at any moment in time. When making mistakes (i.e. violating the 'norm'), this individual can be punished (i.e. cut off the internet) or re-trained via online platforms.

Focusing on the new, biopolitical mode of power, Foucault (2003: 246) predicted the use of 'forecasts, statistical estimates, and overall measures' as means of biopolitics and this is exactly what big data software and satellite imagery provide. Drones, satellites and social media, moreover, can give information about the man-as-species (i.e. the mass). These tools are, for instance, used to monitor and govern refugee camps, migration flows and informal settlement patterns. In short, technologies further enable the biopolitical power over beneficiary communities and, therefore, make their lives even more dependent on general, regulatory decisions. In other words, due to technological progress, aid agencies' power over the lives of beneficiaries is further centralized and easier wielded than ever before.

Beck's perspective

As Beck (1992: 19) described, techno-scientific development is an essential process of modernization. Risks to this development are constantly managed in modern societies to prevent the risks to techno-scientific development from exceeding the threshold of tolerability. Following Beck's view, there may be various challenges to the use of new technologies for aid, but these will not be able to reverse or even halt this modernization process. Beck's theory seems to be confirmed in practice since aid agencies continue to test, adjust, adopt and use technological innovations.

Following Beck's predictions, however, these technologies come with new risks as well, since technologies may fail or be used for malevolent purposes. As a result, aid agencies resorting to technological innovations are constantly adjusting their systems to prevent new risks and will continuously have to implement new measures to enhance the resilience of the existing systems. Examples of aid agencies' attempting to enhance their technological resilience are abundant. For instance, in order to be able to communicate and gather information, devices need power. In places where electricity is unreliable, solar panels and wind energy are used as resilience-enhancing solutions (Interview 12). Building in anti-malware and anti-hacking software in the agency's computer is another example of increasing technological resilience (EISF, 2010). Thirdly, automated techniques can filter out false Tweets and pictures online, making big data analysis a more reliable source of information (Gupta, 2013), while advancements in Artificial Intelligence help to process and analyze large numbers of Tweets and messages with fewer mistakes (Meier, 2015a). Lastly, Broadband Global Area Network is used as a back-up for failing internet connections (Interview 25).

Politicization of aid

Although the usage of aid for Western security or political interest is not hugely affected by the rise of technological developments in the aid sector, technologies contribute to the image of aid agencies as inherently Western, since most of the employed technologies have their origins in Western industries or militaries. This also explains the suspicions of armed groups, including Al Shabaab and the Taliban, that technological tools as GPS coding and smart phones are used for Western political purposes, such as espionage (Interview 2 & 31). In addition, the increased efficiency and effectiveness of aid due to technologies can be seen as an essential element of pursuing Western security interests. In this line of thought, technological developments enable and improve fast and appropriate responses to crises in the world and, thus, reduce potential security threats to the West.

Militarization of aid

In its daily operations, the aid sector is frequently implementing 'military' tools and mechanisms (i.e. tools and mechanisms which originate in the military) (see Sandvik and Lohne, 2014), some of which may lead to unwanted connotations between aid and the military (Interview 2 & 29). Admittedly, many technologies that aid agencies have implemented in the past have their origins in the military (e.g. satellites), but it is hard to find historical resemblances to the challenges that current technologies pose to the aid-military nexus.

Firstly, although not being flawless, current technologies are increasingly able to 'humanize' warfare (see Sandvik and Lohne, 2014). While previous technologies were focusing on scaling up the destruction, drones can quite precisely eliminate specific targets. This raises the very hard question whether aid agencies need to support very precise military interventions in order to protect themselves and populations against future attackers or whether they stay neutral and reject any military intervention but face an increased risk of being attacked by a malevolent actor.

Secondly, new technologies enable aid agencies to witness humanitarian crimes *as they are perpetrated* (see Ibid.), which raises the difficult question whether aid agencies should intervene to protect, for instance, civilians under threat. This would, most likely, mean sacrificing the humanitarian principles and resorting to (military) interventions. The dilemma that aid agencies will probably soon face, is that they either need to support military interventions to protect civilians under threat (which impinges upon their ideals of impartiality and anti-militarism) or they will have to allow these crimes against humanity to be committed (and fail to protect vulnerable populations while having the means to do so). In short, the 'humanization of war' and the ability to intervene (military) in order to protect communities against imminent violence as well as the military connotation of many technologies blur the distinction between aid and the military and pose some pressing questions.

Virtual realities

The rising use of technologies enables the increasing remoteness of expatriate staff from the field. This detachment from the field has unwanted social, emotional and psychological effects (Duffield, 2012). Since cyber-humanitarianism transforms aid in a virtual reality (Donini and Maxwell, 2013), the visualizations that international staff makes or gets presented, lose their relation with the tangible, physical realities of the field. In other words, technological visualizations of large swaths of data may give a fast and clear idea of the 'facts', but the absence of the field prevents a contextual frame which could provide nuances to the 'facts' or, at the very least, could embody what has been measured. In other words, improved knowledge does not necessarily lead to an improved understanding. In addition, although the distance from the field reduces the chance of making bad decisions by being swept along or by being overwhelmed by emotions, the virtual reality of aid provision is likely to lead to less empathy on behalf of the remotely located staff as well as less equality between the provider and receiver of aid (Ibid., Sandvik and Lohne, 2014).

Commercialization of aid

Because the implementation of technologies often requires technical know-how and advanced systems, aid agencies are increasingly collaborating with private partners. The United Nations, for instance, collaborates with the Vodafone Group Foundation for developing telecommunication systems, implementing data systems and promoting research on how technology can be used for humanitarian purposes (UN, 2008). Medair has partnered up with Qlik, a business analytical company that developed a tool that can combine and analyze multiple datasets in one analysis, which greatly improves Medair's assessment and analysis capabilities (Interview 29). With the continued rise of technological innovations, these partnerships will likely occur more and more frequently.

Due to the increasing partnerships between aid agencies and for-profit actors, the line between the two actors is blurring. One of the most striking findings in this regard is the frequency with which aid agency representatives refer to their organizations as (humanitarian) businesses (e.g. Interview 12 & 23). Exemplary for this process is the rising competition between aid agencies. Since information and communication technologies improve data exchange and thus the (popular and donor) oversight over the activities of aid agencies (see Interview 30), aid agencies are more and more behaving as companies that need to show 'good results'. The fierce competition over funding and donations shows remarkable similarities with the competition over customers by companies. This leads to situations in which a glorified self-image takes precedence over sector-wide learning and inter-agency information-sharing (e.g. Interview 28). As a worrying example, security incidents are filtered out in order to keep up the image of the agency (Interview 21).

Conclusion

In short, technologies can result in great and valuable benefits for aid delivery in conflict settings. It can make the delivery of goods and services more efficient and effective, whereas the visualization opportunities can improve information exchange. Technologies may also have democratizing effects. In contrast, especially in conflict settings, opposition can be expected, both from within and outside of the agency, while certain conditions need to be fulfilled before technologies can be implemented successfully. Moreover, technologies can have negative effects on equality and data reliability. Nevertheless, aid agencies try to find and have discovered ways to deal with these challenges. On a more theoretical level, from a Foucauldian perspective, the rising use of technologies enables better biopolitical control over populations, while Beck states that new technologies will constantly introduce new risks and, thus, will continuously require new resilience-enhancing efforts. Further, technologies politicize aid by contributing to the image of the aid sector as Western and by making the aid sector's political goals more easily reachable, whereas new technologies both blur the lines between aid and the military and lead to some new, unprecedentedly pressing questions. Also, technologies transform aid into a virtual reality, detaching international aid workers from the field which results in reduced understanding and empathy. Lastly, technologies have led to new partnerships and fierce competition among agencies, which commercializes aid provision. Regardless of these challenges, the technological revolution will undoubtedly continue and fundamentally change aid delivery in the foreseeable future.

Chapter 4: Risk perceptions and security management approaches

Risk perceptions in the aid sector

In order to understand how aid agencies manage the risks in their environment, it is essential to known which risks are being perceived by aid workers. As Collinson and Duffield (2013) report, aid agencies are increasingly worried about the risks in their environment. Risks for aid agencies may originate in various sources, varying from simply their presence in a conflict area (related to the risks of collateral damage) to the local political dynamics (causing risks of revenge out of discontent). It is worthwhile studying the risk perceptions of the aid agencies as well as which threat sources and risk levels are distinguished by actors in the field before discussing their approaches to these risks.

The wide range of applicability possibilities of technologies means that new technological tools and methods can be used for varying purposes, including malicious purposes. For instance, armed groups can use the internet for spreading propaganda, while criminals may use their laptops and online experience to hack into the electronic systems on which aid agencies rely (EISF, 2010). In short, malevolent actors and belligerent parties use technologies as well. As part of the description of the risk perceptions of aid agencies, it is therefore important to highlight the (future) risks of technologies when they are being employed by actors with malevolent intentions.

Risk archetypes

Collateral damage

Aid agencies report that one of the main risks that they face, is the risk of falling victim to the violence in their environment without being actively targeted. In other words, they are not vulnerable because an actor is intentionally trying to harm them. Rather, they claim to be mostly (or, in some cases, only) victimized by accident. This means that they are the collateral damage of an attack. Security managers and country directors alike refer to this risks as the risk of being 'in the wrong place, at the wrong time' (e.g. Interview 15, 16, 23, 24 & 25).

Roughly two types of collateral damage can be distinguished. Firstly, aid workers frequently fall victim to random shells, stray bullets and artillery duels, due to 'mistakes' by either of the belligerents (Interview 7) or the 'carelessness about how they apply fire' (Interview 21). The conflict in Syria, for instance, involves some thousand different armed groups, some of which target populations indiscriminately and thereby pose a high risk to aid workers (Interview 7). Likewise, in South Sudan artillery is of questionable quality which makes aiming difficult and therefore often unintentionally harms aid workers (Interview 21).

Secondly, conflict environments tend to be contaminated by weapons. Next to collateral damage as a consequence of active fighting, aid workers may suffer incidents from the presence of IEDs, booby traps and (land)mines (Interview 8, 22 & 23)[4]. The bad quality of artillery and shells in South Sudan, for example, leads to the presence of many Unexploded Ordnances. These remnants of war may cause victims among aid workers that happen to be hit when the explosives finally do explode (Interview 19).

Armed groups and terrorism

Aid agencies do not only perceive risks from unintentional violence, but also consider themselves as being targeted in the most volatile countries of this world. A main source of threat to aid agencies in this respect are armed (opposition) groups, including loose gangs, fragmented splinter groups (Interview 6) and freelance militias (Interview 23). Although aid agencies generally try to avoid a confrontation with these actors (e.g. Interview 6), the large number of armed groups and armed individuals as well as their relative anonymity make it hard to predict if, when and where they will strike (Interview 2 & 7).

[4] Personal communication, INGO Country Director

The intentions of an armed group to commit an attack on an aid agency vary. Their attacks can be a means to transmit their opposition against the presence of an international organization (Interview 2) or an attempt to attract visibility (Interview 12). In traditional conflicts, targeted attacks can also be a result of the war dynamics, for instance when the army carjacks vehicles in order to transport its troops. It may also stem from suspicions of aid agencies' support for the government (Interview 4 & 5), especially in case an agency has accepted politicized or government funds (Interview 27 & 31). Lastly, armed groups may intentionally harm aid workers out of a sheer lack of understanding of the work that an agency does (Interview 7).

Terrorist groups, as a subset of armed groups, are frequently identified as threat sources by aid agencies operating in areas in which these groups are active. Their lack of respect for the humanitarian space makes them primary sources of risks (Interview 22). Terrorist groups, such as the Taliban in Afghanistan (Interview 1 & 25), ISIL in Syria and Iraq (Interview 11 & 22) and Al Shabaab in Somalia (e.g. Interview 10 & 13), limit humanitarian activities by threatening or obstructing aid actors. Since terrorist fighters do not necessarily aim to preserve their lives (while security systems are built on this assumption), terrorist attacks tend to be very deadly (Interview 30).

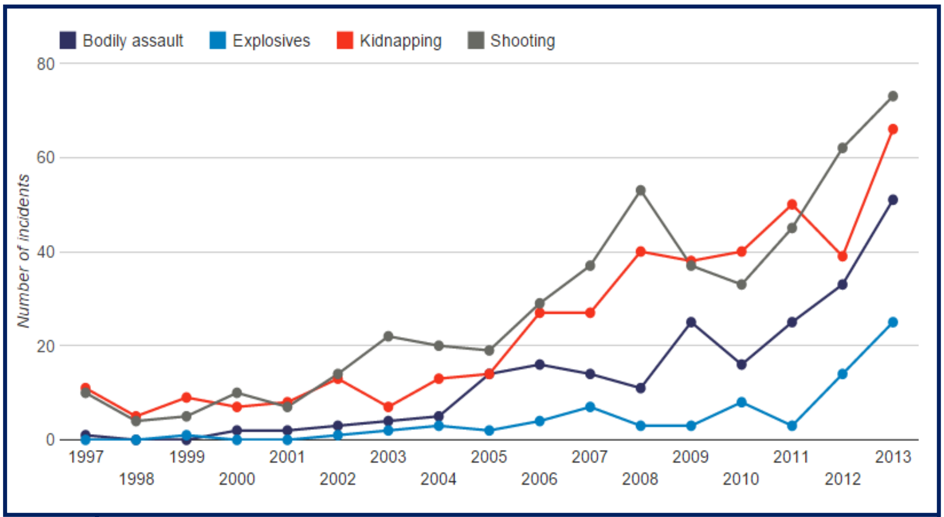

Figure 6: Methods of intentional violence against aid workers (Stoddard et al., 2014)

Methods of armed groups include rocket and mortar attacks, drive-by shootings, IEDs, sniper shootings and assault on compounds (Interview 8). Possibly the most popular method among armed groups, however, is kidnapping (or abduction), which is used in more than a third of the attacks on aid workers (Harmer et al., 2013). Although the risk of kidnapping is higher for expats, national staff cannot be assumed safe (Interview 2) and even peacekeeping troops are not immune (Interview 9).

Local politics

Aid agencies claim to observe the humanitarian principles of impartiality, neutrality and independence, whilst operating in conflict areas. Nevertheless, the humanitarian space (or, alternatively, the humanitarian arena) in which they operate, is in fact highly politicized (Hilhorst and Jansen, 2010). The effects of aid delivery can significantly affect local-political relations in various ways. When the use of violence is the accepted method for solving a disagreement or problem (Interview 4 & 28), aid agencies will inevitably face serious risks.

The most prominent example of this type of risks is related to ethnic and clan issues. While the aid agency itself may not be targeted in ethnic conflicts, its staff may be at risk due to their ethnicity (Interview 16 & 19). The agency will only become a target when it is perceived to unfairly benefit one of the ethnic groups or clans. When there are suspicions of unfair distributions or the perceived neutrality is compromised by an aid agency's (lack of) support to a certain group, the risks of an attack will rise (Interview 17 & 27).

In areas where ethnicity and clans are the prominent means for social ordering, 'ordinary' activities related to Human Resources and logistics are very precarious. Every time a person is hired or fired and whenever products need to be bought, the local clan or ethnic dynamics are to be closely considered (e.g. Interview 5 & 13). Incautious procedures or a neglect of a clan's concern will most certainly result in a violent response. In Somalia, for instance, clans will typically throw a hand grenade into a compound to send their message of discontent (Interview 4).

Crime

A last explanatory factor for violence against aid agencies is to be found in their wealth. Because of their relative wealth, criminals are prone to target aid agencies and aid workers. Criminal activities flourish in conflict areas since lawlessness reduces the chance of prosecution. Criminal groups and individuals use various strategies for illegally apprehending resources. Again, kidnapping is a popular method (Interview 2 & 7). Kidnapping for ransom can be carried out by various actors, including pirates, clans and freelance militia, but armed escorts, which are hired to protect aid workers against abduction in the first place, are also frequently involved in kidnappings (Interview 4 & 23). In Somalia, there are also signals that kidnapped individuals are sold to Al Shabaab (Interview 23).

Another method that criminals use, is the theft of financial and material resources from aid agencies. The increased availability of small arms is reported to enable these crimes (Interview 27). One of the most prevalent crimes is the theft of cars (i.e. carjacking), meaning that there is a high risk to car ownership in, amongst others, South Sudan and Somalia (Interview 4 & 8)[5]. Lastly, criminals may break into a compound and loot aid agency assets. For example, just after the South Sudanese civil war broke out, 'hundreds of metric tons of food stuffs and what not were looted' by various parties to the conflict (interview 21). As a result of the wide prevalence of criminality, governments sometimes try to limit aid supplies out of fear they may be stolen and used by the other party (Ibid.).

Risk perceptions disentangled

Risk perceptions by context

The two main risks, identified by aid actors in Somalia, are the presence of Al Shabaab and the clan dynamics. Al Shabaab has only singled out the UN as a target (Interview 10, 12 & 13), so other agencies report that they are generally safe from Al Shabaab as long as their signals are observed (Interview 6). This means, for instance, that aid agencies cannot send expatriate staff into Al Shabaab controlled areas, but need to stay in the government-held cities (Ibid.). Clan dynamics, however, threaten all aid agencies. The clan struggles over resources, in combination with the use of violence as a means of conflict resolution, make Somalia (in relative terms) the most dangerous place on earth for aid workers (Interview 4, 14, 20 & 23). It is worthwhile to add that the risks vary per region (e.g. South Central Somalia is far more dangerous than Somaliland) (Interview 4). Lastly, in contrast to most other active conflict areas, the rural areas are more dangerous than the cities for aid actors (Interview 23), mostly due to Al Shabaab fighters' presence in these rural areas.

Iraq's security managers and country directors mention that the main risk to their staff and activities is caused by (potential) collateral damage (Interview 24). Belligerents make use of war shells, rocket attacks and IEDs, all of which can bring harm to aid workers (Interview 8). In addition, there is a lot of random bombing in Iraq's capital city, Baghdad, rendering the city a 'no-go' area for international staff (Interview 16). Targeted attacks, however, are either taking place in ISIL-areas (which are therefore usually avoided) or are due to the ethnic background of local staff but pose no risk to the aid agency at large (Ibid.).

The conflict in Syria creates a very challenging environment to aid actors due to its incomprehensible complexity and the extreme fragmentation of the belligerents participating in the fighting (Interview 7). Except for ISIL, most armed groups seem to respect the humanitarian space, although the kidnapping of expatriate staff and the abduction of UN troops highlight the uncertainties for the aid

[5] Personal communication, INGO Country Director

sector in this respect (Interview 8 & 22). The size of the fighting means that collateral damage is a serious risk as well, with some groups targeting areas indiscriminately (Interview 7 & 22).

Aid agencies in Afghanistan, the most dangerous country for aid workers in absolute numbers (Stoddard et al., 2013), face risks of many armed actors and groups, most notoriously the Taliban (Interview 1 & 2). The Spring season, when the Taliban regroups and convenes, introduces traditionally the most risky season (Interview 25). Abductions are a common practice in Afghanistan, but in areas which are not controlled by an established party, aid workers are even more likely to be kidnapped (Interview 2). The many coexisting conflict factors (e.g. political rivalries and ethnic tensions) as well as the number of insurgency groups lead to grim prospects for the security of aid worker staff in Afghanistan[6].

In the case of South Sudan, uniquely, international staff members are perceived to be at lower risk than their national counterparts. The master cleavage between the government and the opposition, roughly split along ethnic lines, results in such high risks for national staff that they can no longer work in areas in which the other ethnic group is dominant (Interview 19 & 21). Internationals, except for Ugandans (due to the Ugandan involvement in the conflict), mostly face risks of collateral damage due to the prevalence of small arms and bad quality artillery (Interview 19 & 21). On the organizational level, hiring and firing staff as well as the theft of food, cars and personal properties may lead to targeted attacks on aid agencies as well (Interview 5 & 21).

Risk perceptions by type of aid agency

The ICRC and its national counterparts, unlike other aid agencies, are willing and trying to find ways to operate in areas that other agencies tend to avoid for security reasons. The Red Cross is, for instance, implementing projects in ISIL-held territories in Syria (Interview 7) and Iraq (Interview 8) and in Al Shabaab-controlled areas in Somalia (Interview 6). Apart from the risk of abduction and risks due to being an international organization, ICRC staff consistently states that the main risk to them is the risk of collateral damage (Interview 2, 6, 7 & 8). As such, the ICRC consistently sees fewer risks and estimates them lower than other agencies in the chosen conflict areas.

The United Nations may exist of various agencies, funds and programs, but its security framework was centralized in 2005 under the United Nations Department of Safety and Security (UNDSS) (Interview 12). With regard to its risk perception, this means that the UN agencies, funds and programs, in theory, follow and respond to one standardized assessment of the risks. Whether the risks are acceptable to a program is determined by an expert panel's assessment of the criticality of every UN project in a country (i.e. Program Criticality). Every project, then, is given a score ranging from one (live-saving) to four (not essential) (Interview 9). Life-saving projects can continue even in very high-risk environments, while less essential projects need to be suspended if the risks rise to a certain level (Ibid.). There is some room for maneuver since high-ranking UN officials may, occasionally, overrule this formal assessment and allow for the continuation of a program or project in volatile times. Similar to their (mathematical) risk assessments, the risk perceptions of UN staff are voiced in a rather formal and scientific manner (Interview 9 & 11), although perceptions of a situation may differ (see Interview 11 and 13). This means that even a standardized assessment does not necessarily lead to a coherent organization-wide view on risks. In general, UN staff members tend to perceive risks as higher than other aid agencies' staff. This, again, can partially be explained by the fact that the risks and threats to the UN are indeed elevated because of its political nature.

NGOs report remarkably uniform perceptions of the risks in the separate environments. Although full-time security managers of large organizations tend to use more formal language and have more examples at hand, the identified threat sources and risk levels are roughly the same. For instance, in Somalia, large and small agencies alike report that Al Shabaab does not pose a significant threat

[6] INGO Country Security Strategy

when you evade their areas or abide by their rules, but they almost all mention that clan-issues (e.g. hiring and firing) can and do pose serious risks (Interview 4, 14, 17, 20 & 23).

Metcalfe et al. (2011: 6) discuss how humanitarian and development actors differ in the way they perceive risks. While the latter are concerned with the risks of intervening, the former consider the risk of not intervening. This results in humanitarian organizations being more risk-taking than their development counterparts. Risk-taking actions by humanitarian agencies are possible because these organizations have shorter time-frames, clearer goals and simpler relations with local actors (Ibid.: 6). In practice, however, this distinction seems not so clear. First off, since a lot of agencies combine humanitarian and development activities (Interview 26), even a relative distinction is rendered unfruitful in practice. Moreover, there does not seem to be a recognizable difference in how these types of aid agencies view risks (Interview 30).

A distinction that resonates better is the distinction between Christian aid agencies and non-faith-based organization. Some aid actors state that Christian agencies face higher risks when operating in a predominantly Islamic context, for instance in Syria (Interview 22), Somalia (Interview 23) and Afghanistan (Interview 25). On the other hand, many of the groups that would harm Christians out of religious belief are also opposed to atheism or to some of the aid activities in general (e.g. empowerment of women) (Interview 1). Whether Christian aid agencies are in fact singled out as targets is therefore open to discussion.

The use of technologies by threat actors

Just like aid agencies, actors threatening them are also increasingly making use of technologies in order to instill fear or use violence against aid actors. For instance, technological progress in military hardware renders weapons more widespread (e.g. Interview 5 & 19) and more deadly (e.g. Interview 9, 12 & 13). The technologies that aid agencies are employing (mostly ICTs) are also turned against them. Malevolent actors' usage of communication tools and undermining technologies can be expected to affect the aid agencies' risk perceptions significantly, although evidence is incidental as of yet. Nevertheless, with the rising use of technologies by threat sources, the influence of technologies on risk perceptions may rise as well, which makes an elaboration worthwhile.

Communication technologies

By using new communications technologies, militant groups can more easily spread rumors and falsities about aid agencies, making it harder to build acceptance and manage perceptions (EISF, 2013). Fabricated information can also spread more easily over online platforms. A related danger is that this false information leads to a vicious circle in which individuals meet like-minded people on online platforms, find their own beliefs confirmed and stir up violent thoughts and actions towards aid actors (Sambuli and Awori, 2014).

Figure 7: Al Shabaab's Twitter-account

Next to spreading false information, communication technologies are used for propaganda purposes. In October 2014, Somali terrorist group Al Shabaab released a video, explaining its motivations to attack the UN compound in the preceding year. The professional video does not just hail the 'martyrs' but also incites hatred against the UN, referring to it as a 'satanic force'[7]. Earlier, the group used Twitter during its siege of the Westgate Mall in September 2013 (Katz, 2014). Similarly, the Islamic State of Iraq and the Levant has uploaded lots of videos and images of its campaigns and used Twitter and Youtube for sending their propaganda message of violence and terror into the world as well as for recruiting new fighters (Ibid.).

[7] Video acquired through personal contacts

The risk perceptions of aid agencies are subject to the online activities of threat actors, most notoriously their propaganda. The first and foremost objective of propaganda (e.g. images, video) is to instill fear, to send a message that both frightens and coerces (Minei and Matusitz, 2012). Spreading panic and fear is even more effective through social media than through traditional media, since the message can reach a wider public and can be repeated over and over again. Propaganda inherently aims to influence perceptions, cognitions and behavior (Ibid.: 167). Therefore, videos that show attacks on aid agencies intend to frighten aid agencies and aim to change their activities. Albeit speculative, aid agencies' absence of Al Shabaab- and ISIL-territories hint at the success of their propaganda campaigns.

Furthermore, governments and armed groups monitor the activities of aid agencies on social media with various consequences. Firstly, social media can serve to identify which individuals are helping aid agencies (e.g. on reporting human rights violations), rendering these collaborators vulnerable to reactive punishment (Interview 11; UNOCHA, 2013: 39). Secondly, online information on the location in which aid workers are (or will be) providing goods or services can be used by actors to thwart aid activities, or even to attack the aid workers as well as those who accept their help (Ibid.).

Interestingly, interagency communication further influences the aid sectors views on risks by improving reporting on and analysis of the attacks on aid workers. Most notably, Humanitarian Outcomes publishes an annual Aid Worker Security Reports since 2011, after two initial reports in 2006 (Stoddard et al., 2006) and 2009 (Stoddard et al., 2009). This data leads security managers to state that the world does indeed become a more dangerous place for aid workers (Interview 26 & 27). Although incident statistics are important for the risk management of aid agencies, these statistics should not be seen 'as providing a robust picture of the actual risks that aid workers face' (Van Brabant, 2012: 14). Nevertheless, they do affect risk perceptions and inform security strategies.

Undermining technologies

Another way in which belligerents or malevolent actors can use technologies to the detriment of aid agencies is by undermining the technological systems on which agencies rely. For instance, some governments and groups have the capacity to intercept private emails, follow someone's online activities after hacking into a computer and trace and tap mobile phones (e.g. by installing spyware on electronic devices) (Byrne, 2014; EISF, 2010). Hacking into supposedly private communication channels undermines the security of aid agencies and can hamper the response in case of security incidents (EISF, 2013)

Next to installing spyware, malicious actors can send viruses to the computers of aid agencies or conduct other cyber-attacks (EISF, 2010, 2013). In case valuable information is destroyed or damaged, the aid agency will face a reduced capacity to respond and will be more vulnerable to physical attacks, especially if security-related information was lost (EISF, 2010). Although aid agencies may not have faced these incidents at a large scale yet, contemporary conflicts are witnessing 'private citizens forming into on-line militia groups to perform cyber-attacks against political opponents' as well as groups that wield 'guns one day and a laptop the next' (Gilman, 2014: 8).

A final set of technologies that undermine existing systems of aid agencies are technologies that simply set off other technologies. For instance, many aid agencies use devices that enable them to track and trace their staff and properties (e.g. Interview 16, 26 & 29). Professional carjackers and criminals, however, are aware of the presence of this tracing equipment and have developed jamming devices, rendering the original technology useless (Interview 27). Even worse, malevolent actors may hack into the system and trace the agency's cars (see Interview 27).

Technologies that tackle the systems upon which aid agencies rely, shape agencies' risk perceptions as well. The (potential) impact of attacks on the underlying systems and the theft or loss of electronically stored information is much higher than ever before, which has resulted in increased attention for digital security (EISF, 2010, 2014). In addition, hacking and jamming devices that undermine existing systems may very well result in the loss of trust in these technologies or even in the trust in technology altogether. In any case, risks can be expected to be perceived higher due to the capacity of threat actors to harm, undermine and hack into these technologies.

Security management in conflict settings

Regardless of the threat's origins, many aid agencies, led by the UN, went through a shift over the last few years in their security management approach. Instead of determining 'when to leave', they now try to find out 'how to stay' in volatile settings (Egeland et al., 2011). The 'duty of care' (i.e. the responsibility for the well-being of staff) becomes more pressing as a consequence and mitigation measures have been put in place to reduce the security risks to aid workers. Before discussing the security strategies and how they are applied by various organizations in different areas, it is worthwhile stressing that the norm of 'how to stay' is applicable to aid agencies' activities in general but not in every specific case. The importance of the activities is weighed against the risks, which means that live-saving programs will almost always continue while less critical projects will be suspended more easily (Interview 9 & 30).

Since the risk can differ for national staff and international staff, security management measures will be different for them as well (Interview 13 & 28). The security manager of an aid agency therefore usually needs to do two different risk assessments (Interview 9). The security manager is largely responsible for choosing appropriate security measures, but the implementation of a selected security strategy depends on the availability of funds. While some agencies face difficulties with funding for security (Interview 27), others recognize an increasing willingness on the donors' behalf to fund security efforts of aid agencies (Interview 26).

Information is key in the formulation of security strategies. Without accurate information on belligerents, their weapons and their view on an aid agency, a strategy risks being useless. This information can be collected from various sources, including from government forces on the ground, other aid agencies, reconnaissance elements, local contacts and media (Interview 9 & 13). On the basis of this information, assessments can be conducted and security strategies formulated. Since information is essential for security assessments, information-sharing on security issues is an important topic of debate in volatile areas. Virtually every security manager and country director, for instance, applauded the work of interagency security fora such as NSP (in Somalia), the South Sudan NGO Forum and INSO (in various countries). Their reporting of incidents, advisories and analyses prove highly valuable (e.g. Interview 1). Nevertheless, information-sharing *among* aid agencies on security issues is mostly informal (Interview 30 & 31) and ad hoc (Interview 15) for various reasons.

The most important reason is that security information is sensitive (Interview 17 & 30). Security incidents can result from ignorance or a mistake which the aid agency prefers to cover up in order to prevent reputation damage (Interview 21 & 31). Also, an aid agency may refrain from sharing security information out of fear of compromising its neutrality or because it would be easily identified as the source (Interview 2 & 21). Furthermore, national staff may hold back security information because it might end a project (and their employment) (Interview 4) or simply because they do not recognize a situation as dangerous since they have a very different idea of what constitutes as a risk due to their background. Lastly, the ambiguous realization of the security information-sharing platform of the UN and NGOs (under the Saving Lives Together framework) means that informal contacts still determine in many areas to what extent information is exchanged between these two types of agencies (e.g. Interview 4 & 25). Challenges aside, there

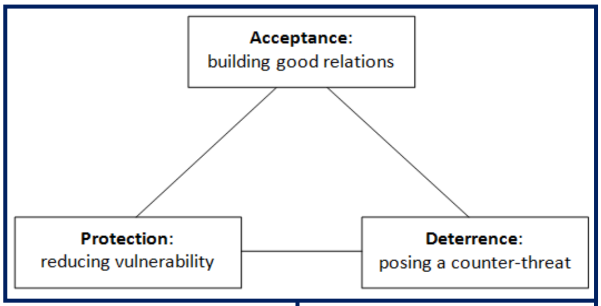

Figure 8: The security triangle

seems to be good security information exchange on the headquarters' level (Interview 27) and when informal contacts between managers are good. This means that aid agencies are, in many cases, well-equipped to make informed decisions on the security strategies they choose to employ. Historically, there have been three security strategies that aid agencies have used. This combination of security strategies is usually referred to as 'the security triangle' (see figure 8).

Security management strategies

Acceptance

The preferred security strategy by aid agencies in conflict areas is 'acceptance' (HPN, 2010). This means that the original risk to an aid agency is reduced or removed because the presence and activities of an aid agency are accepted in the environment (Ibid.: 55). A prime way of building acceptance is creating strong relations with the local communities and authorities by informing them about the aid agency and involving them in the project (Interview 2, 8, 16 & 24). An aid agency, for instance, can work with the local elders (Interview 20) or with a local NGO (Interview 18), while hiring locals does not only lead to better situational awareness but also helps the agency to transmit messages to communities (Interview 28). Alternatively, aid agencies can follow the signals of armed groups (Interview 6), liaise with ground forces (Interview 3) or communicate with armed actors through the communities in which they work (Interview 25) in order to get assurances of security from potential threat sources (Interview 9).

Careful profile management is considered necessary to make the acceptance approach succeed. Thus, observing the humanitarian principles is seen as an essential element of the acceptance approach[8]. By providing high quality services and due to the visibility of the benefits of aid, agencies report good relations with their beneficiaries (Interview 1, 14 & 23). Next to the principle of 'humanity' (in the form of good quality aid), the other humanitarian principles to be observed for building acceptance are neutrality, impartiality and independence (Interview 2 & 6). Moreover, transparent processes (Interview 7 & 20) and context-sensitive behavior of staff further contribute to the acceptance strategy (Interview 8). Since trust is built up over time, profile management will only materialize after the aid agency has been embedded long enough (Ibid.).

Although acceptance is the preferred strategy by aid agencies, it is also insufficient in many context (HPN, 2010). Criminals and armed actors alike have strong incentives to either exploit or refrain from accepting the aid agency's presence. For instance, acceptance will not stop terrorist groups since these groups have a religious or political goal that transcends all other goals (Interview 30). They are often not part of a recipient community either, but rather enter an area where an aid agency is already operating, which means that the acceptance strategy did not include these actors in the first place (Ibid.). In areas with much active fighting, stakeholders are frequently changing anyway, which hampers the acceptance strategy as well (Interview 5). Lastly, when a project nears its completion, communities have less to lose and, therefore, the acceptance strategy is less likely to provide security (Ibid.).

Another, more theoretical, challenge to acceptance is that 'acceptance' is a typical example of a term that is subject to interpretation as well as to personal and mental constructions. Interpretations of and discourses on acceptance vary significantly between different aid agencies. In this regard, the Red Cross, for example, takes a very different approach than NGOs and the UN (Interview 6). Whereas the ICRC aims to be accepted by an entire society, the UN focuses specifically on authorities and NGOs tend to search for acceptance among their target communities. A related difficulty is that acceptance may require choosing sides and, thus, sacrificing neutrality, one of the humanitarian principles. In short, although acceptance may seem the best strategy in theory, its implementation is

[8] INGO Country Security Strategy

often hampered in practice. As a consequence, in volatile settings, aid agencies often employ alternative strategies in addition to the acceptance strategy (HPN, 2010).

Protection

A second approach that aid agencies use to increase their security is 'protection'. This means that devices, materials and procedures are implemented which reduce the vulnerability of the agency (or, in other words, 'harden the target') (HPN, 2010: 55). The reduction of vulnerability is attained in two ways. Firstly, aid workers are protected by reducing their exposure to sources of threats. Secondly, aid agencies increase their protection by reducing the effects of a possible attack.

In terms of reducing the exposure, a few sets of measures can be distinguished. The first set of measures tries to reduce the exposure by limiting the field presence. This can be achieved by setting limits on movements (e.g. traveling by plane instead of by car), reducing the number of people in a region (i.e. relocation), in the country (i.e. evacuation) or in the field (e.g. hibernation or working from home) and by reducing the areas of operation (e.g. avoiding war areas) (Interview 6, 7, 11, 12, 13, 14, 20 & 24). The ability to manage increasingly more parts of the project cycle from a distance by using technologies (i.e. Remote Management) has become a very popular example of this type of exposure reduction. Remote Management is therefore, by nature, a protection strategy.

The second means to reduce exposure is by going unnoticed (i.e. 'low profile' approach) (Interview 5, 18 & 23). By using a Toyota Corolla in Afghanistan, the most common vehicle in the country, and not advertising one's activities, aid agencies may go rather anonymously (Interview 1 & 18). This strategy is particularly applicable to local staff from the area that easily blend in and refrain from being open about whom they work for, even if this means that their relatives are unaware of their employment (Interview 13 & 17). As a final strategy to reduce the exposure, aid actors can push off their problems to others. For instance, by renting a car in a criminal environment, a carjacking becomes the problem of the original owner (Interview 4). Similarly, by involving the Ministry of Labour in hiring and firing, the risk of revenge is lower since part of the risk is passed on to the ministry (Interview 5).

When these measures fail, aid agencies still have means to reduce the impact of an attack. Some protection efforts are very basic and do not need any technological know-how. Aid agencies use, for instance, sandbags (Interview 6), barbed wire (Interview 2), tight access controls (Interview 27), escape routes (Interview 23) and (unarmed) security guards (Interview 6, 8 & 15). Other measures, however, are the product of technological progress, such as armored vehicles (Interview 7, 12, 15, 28), blast walls (Interview 8), bomb gates, anti-ramming barriers, anti-blast protection (Interview 23) and video surveillance[9].

A final and unique way of reducing the impact is by providing security trainings to aid personnel. These trainings can vary from awareness trainings for field staff to security courses for senior management (Interview 2 & 30). Security trainings can be given by external providers, such as the Centre for Safety and Development and RedR, or they can be designed and provided by NGOs themselves (Interview 5, 26 & 31). Although national staff may face higher risks by working for an aid agency (Interview 28), security trainings tend to focus on international staff (Interview 30). This may be explained by the fact that some national staff members are hard to reach (e.g. in Syria) (Interview 26). Trainings are also less effective in dangerous settings, so an optimal training requires a temporary relocation of staff to a safer area (Interview 30). After a security training, staff needs to continue to be aware of the risks of their environment and, thus, observe the protocols. For this purpose, frequent Rest and Recovery-trips are useful to keep staff focused (Interview 1) and various compliance mechanisms can be used in cases protocols are neglected (Interview 16).

[9] INGO Country Security Strategy

Deterrence

The least preferred security strategy that aid agencies (have to) use, is the 'deterrence strategy'. This approach means that the aid agency poses a counter-threat (HPN, 2010: 55). The least aggressive measure of deterrence is the threat of withdrawal (Interview 19). When the aid sector is in danger, an aid agency can pull out on its own (Ibid.) or collectively (Interview 5). The latter strategy prevents the possibility of one or a few agencies being singled out as the culprits (Interview 5). Alternatively, an aid agency can scale down instead of leaving altogether[10], whilst it can also temporarily stop the delivery of aid (i.e. suspension) (Interview 16).

In extremely dangerous environments, aid agencies have resorted to the use of armed escorts and armed guards, either against criminality (Interview 4, 6 & 23) or against terrorist groups (Interview 10 & 13). While other agencies rely in this regard on private security providers, the UN now also has its own guard units, which are troops that are provided by Member States and which are tasked with the provision of security to UN civilian personnel. They are not part of UN peacekeeping missions as this would mean a reduction of troops for the implementation of the mission's mandate. These troops are also based in countries without a UN military presence, such as Somalia (Interview 9 & 11).

Implementation of security strategies per context

Afghanistan

In Afghanistan, as the most dangerous country for aid workers in absolute terms, aid agencies rely heavily on protection mechanisms, including traveling by plane, improving compound security and security trainings for all staff (Interview 1 & 2). In many cases, agencies also operate with a low profile (e.g. by using the unnoted Toyota Corolla instead of a white Land Cruiser) (Interview 1). Whether it is advantageous to go in with a high profile (e.g. including the aid agency's flag) or at a low profile depends on the volatility of the province (Interview 25). The UN, however, is mandated to keep a high profile and (therefore) relied or relies on the deterring power of armed private security companies (Interview 9 & 11), while NGOs and the ICRC generally refrain from using (armed) security companies.

The acceptance strategy, as it is (limitedly) employed in Afghanistan, seems to be double-layered. First and foremost, agencies seem to focus on assuring that they are not attacked by any of the armed actors, including the Taliban, by talking to them directly (Interview 2) or indirectly via local village elders (Interview 25). Secondly, one security manager also emphasized the importance of building acceptance among the local communities by continuing the dialogue and by observing the humanitarian principles (Ibid.), while a country director mentioned that its projects led to good relationships with local communities (Interview 1). The overall strong reliance on protection is probably due to the historically close collaboration with Western militaries as well as to the many coexisting conflict factors which create a broad array of risks that agencies perceive and, subsequently, aim to mitigate.

Iraq

In the case of Iraq, it is worthwhile noticing that virtually every aid agency is only or mainly working in the Kurdish areas in the north. This fact, in itself, is already exemplary for the wide use of protection measures, which is one of the two main strategies in the country. Aside from the use of armored vehicles (Interview 11), blast walls and unarmed security guards (Interview 8), security protocols (Interview 16) and a tight control of movements (Interview 24), security trainings are an essential part of the protection strategy in Iraq (Interview 16 & 24). Within the (safer) Kurdish areas, acceptance-building measures are employed by sharing information on projects and on the aid

[10] Personal communication, INGO Country Director

agency (Interview 8), by informing communities through local contacts, by asking for permission to visit them (Interview 16) and by consulting the government (Interview 24).

Uniquely, security managers and country directors in Iraq share security information more freely and seem to be more satisfied with their collaboration than elsewhere. Firstly, the work of INSO, which shares security information and does analysis, is well-received (e.g. Interview 16). In addition, there is information-sharing between NGOs via Skype, a system set up by a security manager of Save the Children (Interview 24). Moreover, the security collaboration between the different types of aid agencies seems very good as well. While the ICRC in Iraq is more open to share information with the UN and NGOs (Interview 8), the latter two have a good working relationship historically (Interview 3).

Somalia

As violence is the established means for conflict resolution in Somalia, it is the only context in which acceptance strategies seem to play a marginal role in the security management of aid agencies. Although building acceptance among clans is necessary to be able to operate in their areas, acceptance strategies mainly focus on being visibly useful to the community (Interview 23) and on working with (local) authorities (Interview 17 & 20). Although the inclusion of all groups (e.g. clans) would be part of an acceptance strategy in other areas, their inclusion in Somalia is rather a protection strategy to prevent being seen as only benefiting one clan and being targeted as a result (Interview 14 & 20).

Other protection measures are the usage of planes for movements, guard units or Special Protection Units (SPUs)(Interview 11 & 20), armored vehicles (Interview 12, 15 & 28) and security trainings (Interview 14 & 17). Also, decision-making power is often centralized to reduce pressure on national staff (Interview 4). Usually, national staff keeps a low profile (Interview 13 & 14). As such, nationals are even able to work in Al Shabaab areas on specific projects when local commanders allow them to do so (Interview 4). Some agencies also make use of armed escorts as a means to deter criminals or splinter factions (by NGOs and the ICRC) and Al Shabaab (by the UN) (Interview 6, 10, 13, 18 & 23). The wide use of protection and deterrence strategies by aid agencies in Somalia fits their perception of the risk environment well. Since violence is viewed as an established means for conflict resolution, agencies see protection and deterrence as a logical response to enhance their own security[11].

NGOs and the UN speak in laudatory terms about the NGO Safety Program in Somalia. Nevertheless, information-sharing on security incidents remains an arduous endeavor. A possible explanation for the restrained way of security information-sharing among NGOs is that the diversity of the conflict drivers makes agencies fear the possible repercussion of sharing sensitive information (Interview 31). While the Saving Lives Together framework yields somewhat positive results (e.g. when evacuation would be needed) (Interview 14 & 23), the physical distance between the UN headquarters in Mogadishu and most NGOs' headquarters in Nairobi limits the collaboration (Interview 13). The location of the headquarters is a sensitive issue anyway. While those located in Mogadishu claim improved understanding of the conflict and more legitimacy, credibility and access (Interview 13 & 15), others refer to the extremely high costs and mention that contact with beneficiaries is also minimal when international aid workers are confined to a bunker in Mogadishu (Interview 17).

South Sudan

After the conflict in South Sudan broke out, the UN was briefly targeted for its alleged support to the opposition, but this has changed. Currently, the aid sector is not perceived to be targeted in the country (Interview 5). Therefore, nowadays, the main security strategy for aid agencies operating in

[11] Sadly ironic, using armed guards in Somalia can, theoretically, also be seen as an acceptance-building measure since it demonstrates a context-sensitive adaptation to a widely used cultural phenomenon, namely deterring threats by posing a counter-threat.

South Sudan is building acceptance through building strong relations with local communities and through providing high quality aid (Interview 19).

In response to the perceived remaining risk of collateral damage, protective measures are still being used. Since importing and transporting protection tools is difficult, most protection measures are quite basic (e.g. bunkers from local materials) (Interview 5). When active fighting breaks out in a certain area, staff can also be temporarily withdrawn from the field through hibernations, scale-downs (to just one person) and relocations (Interview 19). Another measure of protection is to base international staff in opposition areas since national staff may be subject to targeting, for instance when one of the belligerents advances (Interview 19). Deterrence measures are rarely used and usually consist of (the threat of) withdrawal (Interview 5), although the UN has hired a private security company when it was targeted early in the conflict (Interview 9).

The collaboration among aid agencies is widely perceived to be quite good. The rise of the NGO forum and interagency networks has improved information-sharing and collective actions, although informal connections remain important (Interview 19). The relation between the UN and NGOs has a somewhat ambiguous history. On the one hand, NGOs want to distance themselves from the UN because of its politicized nature. On the other hand, NGOs cluster around UNMISS locations, in which there are many IDPs. Until recently, many NGOs even relied heavily on the UN security system (Interview 21). This ambiguity leads to a situation in which UNMISS would be called upon for an evacuation but it would not be allowed to take a lift in a UN car (Interview 19).

Syria

Acceptance is being used in Syria by aiming to transparently deliver high quality aid services and by providing information about the aid agency (Interview 7 & 22). Nevertheless, many actors do no not know or respect the humanitarian space. In the chaos of the Syrian conflict, the success of deterrence is debatable as well. On the one hand, if an aid agency withdraws, it might turn the community against the armed group that harmed the aid agency (Interview 22). On the other hand, terrorist groups usually do not have (strong) ties with the local community and do not seek the support of a community anyway (Interview 30). In practice, the strategy is therefore not widely used.

In short, the most frequently used strategy by aid agencies in Syria is protection, which seems to fit the enormous complexity and scale of the conflict best. In response to the perceived threatening and targeting of aid workers, agencies hibernate, relocate, evacuate and suspend. For instance, after the kidnapping of World Vision staff, the agency suspended its activities in ISIL-areas. In addition, the UN has negotiated for one-day ceasefires in order to provide as much aid as possible in one single day (Interview 9), while on other days, UN national staff works from home (Interview 11). Also, for security reasons, areas of operations, movements and the number of staff in the country have been limited (Interview 7).

The UN has been criticized for its response to the Syrian crisis. The management and coordination mechanisms which the UN provides elsewhere, are virtually absent in the Syrian response (Interview 22). This was partly due to Turkey's unwillingness to allow the UN to get an office for the Syrian response in Turkey which delayed the UN's arrival in the country with more than a year after the NGOs had arrived. This meant that NGOs had already organized their security set-up themselves and the UN became redundant in this regard (Interview 3). The fact that some UN programs are still being run from Damascus complicates the situation even further (Interview 22).

Use and interpretation of strategies by actor

NGOs

The security management strategies of NGOs highly vary per context and per NGO. Nevertheless, a few general deductions can be made. Firstly, aid agencies generally claim that the acceptance approach is their preferred security strategy. This strategy can take various forms, for instance informing local communities and local authorities (Interview 16), consulting the government (Interview 24) or, simply, delivering high quality aid (Interview 14). NGOs, in general, seem to put more effort in trying to be accepted than the UN, but not as much as the ICRC, since NGOs usually refrain from attempting to be accepted by armed groups but simply focus on target communities.

Secondly, regardless of the merits of acceptance strategies, protection mechanisms proved to be a necessity for all security managers and country directors in the countries of this study. Every NGO used protection tools, varying from escape routes (Interview 23) and keeping a low profile (Interview 4) to security guards (Interview 20). In comparison with the UN, NGOs are usually more conservative in their use of guards and armored vehicles, partly because it impinges on their acceptance strategy and partly because there are financial constraints.

Thirdly, the main deterrence strategy employed by NGOs is (the threat of) withdrawal, either on their own (Interview 19) or collectively with other NGOs, such as in South Sudan where it is enabled by the good networks in the country (Interview 5). The use of armed escorts and armed security by NGOs is only to be found in Somalia, where deterrence is used to such a degree that NGOs risk to become militarized (Interview 4). Nevertheless, in most areas, regardless of whether there is a close historical relation between aid agencies and the military (e.g. Afghanistan and Iraq), many NGOs prefer to use protection measures (such as keeping a low profile) and refrain from using deterrence measures.

With respect to their security management strategies, both the religious divide and the distinction between humanitarians and multi-mandate aid agencies do not provide relevant outcomes. However, a distinction on the basis of the size of the aid agency does lead to some interesting insights. Since larger aid agencies tend to have full-time security managers, they are more likely to share security information among each other and cooperate on security issues than their counterparts of smaller agencies (Interview 19 & 23). In addition, bigger aid agencies allegedly better equip their staff. While smaller aid agencies may face organizational and financial challenges, larger organizations can, for instance, more easily provide staff with (in-house) pre-deployment trainings to prepare them for a volatile setting (Interview 21). Since security tools can be very costly, larger agencies are more likely to be able to afford these protection tools as well (Interview 15).

UN

Since the UN works, to a large extent, through and with governments, the classic idea of building acceptance among competing factions or with populations is rendered impossible or useless. The UN, as a political entity, cannot be neutral since its mandate requires political interference. Thus, while other aid agencies try to be accepted as well-intended actors in order to deliver their services, the UN merely aims for acceptance of its service delivery (i.e. access) (see Interview 9). The other two security strategies are fit into the UN Security Management Framework as applicable.

Irrespective of the UN agency, fund or program, the security management is unified under the Department for Safety and Security (Interview 12). Protection decisions, such as suspension, relocation and evacuation, depend on the mathematical risk assessment and the calculated criticality of a program (Interview 9). If risks rise above a certain level, remaining staff is protected by peacekeeping staff or guard units (Interview 11 & 13) and by reducing the exposure through, for instance, traveling by UN planes (Interview 10).

Although the risk assessment and program criticality are calculated with a (computerized) digital tool, the UN's security management still tends to be reactionary. For example, after the UN was hit by an IED in Mogadishu in late December, 2014, the immediate response was to lower the exposure by reducing the number of people and movements (Interview 12). Something similar had happened after an attack on the UN compound in 2013 (Interview 13). However, as long as there are live-saving programs to be implemented, the UN will use protection and deterrence measures in order to stay.

ICRC

Unlike the other aid agencies, the ICRC bases its acceptance approach on talking with all the parties in a conflict, assuming this is possible. The ICRC's acceptance approach therefore involves informing the communities as well as belligerents about its role, mission and goals (Interview 7 & 8). Since neutrality is its cornerstone, ICRC staff aims to avoid being seen with employees from the UN or NGOs that are perceived to be partial (Interview 2 & 6). Due to being long embedded and having build trust over time, the ICRC emblem may be used for protection as well (Interview 8).

Nevertheless, ICRC staff is also victimized and so, protection mechanisms are adopted. Protection measures are mostly used against collateral damage and varies from avoiding the road (Interview 2) and using blast walls and unarmed guards (Interview 8) to using armored vehicles and limiting movements (Interview 7). In Somalia, uniquely, armed escorts are used against splinter factions and criminality (Interview 6), but the ICRC generally refrains from deterring measures.

Risk perception and risk management in relation to social science theories

While Beck (1992: 19) argued that techno-scientific developments would be the main cause of risks in modern societies, collateral damage was perceived to be the primary source of risks to agencies in the volatile borderlands of this study. Nevertheless, the 'modern' aid agencies' responses to these risks closely follow Beck's predictions since they aim to rationally prevent and minimize risks so that aid delivery (which from Beck's perspective could be seen as a means to protect modernization processes) can continue without the security risks exceeding the threshold of tolerability. The strong reliance on the protection strategy is exemplary for the preference for precautionary measures. Whereas some agencies are progressively rationalizing their protective security management (e.g. Interview 19), others, following Duffield's (2012) forecasts, internalize these risks by 'potentially accepting more risks than they should' (Interview 13) and use the instability of their operating environment for furthering modernization processes.

The violence of armed groups and terrorists against aid agencies can best be explained by the perceived politicization of aid. In this view, aid agencies have become instrumental to securing the safety of Western interests by providing relief in conflict areas is. Aid has thus become a means for political purposes (Duffield, 1997; Collinson and Duffield, 2013). In practice, in Somalia, various agencies were perceived to follow an anti-terrorist agenda which resulted in expulsions and targeted attacks by Al Shabaab (Interview 4), while for the Syrian response, the large sums of aid to the region were explained by the fear of large refugee flows to the West (Interview 3). It is also no surprise that the UN, as the most politicized aid agency, perceived and faced higher risks than non-politicized NGOs and the ICRC (e.g. in Somalia). Security management, from this point of view, becomes an attempt to protect the political interests of the West by enabling continued (politicized) aid delivery.

The rise of integrated missions, as a form of the politicization of aid, did not lead to higher perceived risks or casualty numbers among NGO aid workers, but it did lead to a false sense of security since the UN was expected to take care of the security of INGOs, which proved not (necessarily) true in practice (Interview 21). In this research, the only conflict area with a UN peacekeeping mission is South Sudan and, indeed, NGOs 'are clustered generally around locations where you find UNMISS' (Ibid.). Also, NGOs in South Sudan viewed the UN more favorably. Whether this closer connection renders them more politicized in the perception of threat sources, remains a question to be answered. In any case, the UN peacekeepers' protection did result in a militarization of aid. This conflation between aid and the military was even stronger in Somalia (where many agencies use armed guards and armed escorts) and Afghanistan (where agencies historically have had a close relation with the international intervention force). The militarization of aid in these two countries may again partially explain the higher risk perceptions of and violence against agencies in these two countries.

Lastly, taking a Foucauldian perspective, many aspects of aid agencies' security management are reminiscent of the 'old power' of the sovereigns which is disciplinary in nature. In a certain way, aid agencies use this old power over their staff members in order to encourage them to act according to their general security management plans and guidelines (i.e. norms). For instance, staff members get clear directions where to go and what areas to avoid (e.g. Interview 6, 7 & 20), they are punished when violating the 'norms' (e.g. Interview 16) and they receive security trainings to guide their activities in the field (e.g. Interview 26 & 30). All these security methods are, in theory, disciplinary attempts to control staff members as 'individual bodies' (Foucault, 2003: 240-243, 252-253).

Conclusion

The four main risks to aid actors are 1) collateral damage, 2) armed groups and terrorism (which can be explained by the politicization of aid), 3) (the outcomes of) local politics and 4) crime. The use by malicious actors of contemporary communication technologies and tools that undermine aid agencies' technological systems create new risks to their staff and assets. Across different contexts, varying clusters of perceived risks are identified. While Somalia (due to the number of threats) and Syria (due to the size of the conflict) are seen as the most dangerous areas, South Sudan and Iraqi Kurdistan are viewed as relatively safe regions. The UN, with its centralized risk assessment system, almost always perceives risks to be higher than other agencies, whereas the ICRC consistently estimates risks to be lower. Among NGOs, neither the expected increase of risks in integrated missions, nor the expected divide between humanitarian and development NGOs, are verified in practice. However, the idea that Christian NGOs face higher risks in predominantly Islamic countries is frequently advocated. These risks are mitigated or managed by various security management measures, some of which remind of Foucault's description of the sovereign's old (disciplinary) power. In areas in which risks are relatively low (e.g. South Sudan and Iraqi Kurdistan), agencies rely mostly on acceptance measures. Deterrence measures, in the form of armed escorts and armed guards, are for NGOs and the ICRC mostly limited to Somalia to deter threats from splinter factions and criminals. The UN also uses armed guards to protect itself against terrorist groups, such as Al Shabaab in Somalia and the Taliban in Afghanistan. The militarization of aid agencies in Afghanistan and Somalia can be explained by the historical close connections between military entities and aid agencies in these two countries. In most contexts, however, as Beck predicted, protection measures are the dominant option. Specifically when there is a broad array of threats (e.g. Syria, Somalia and Afghanistan), protection mechanisms, through reducing exposure and impacts, are preferred. Since the UN perceives risks to be higher, it is not surprising that its security strategies are more protective and deterring. Similarly, the ICRC, which has a tendency to estimate risks to be lower, invests more in acceptance measures than most other agencies. NGOs take a middle position, but large NGOs seem to be better positioned to provide protective security to their staff.

Chapter 5: The use of technologies in security management

Technologies used for security management

Security management strategies benefit from technological progress in multiple ways. New technological tools, for instance, make security management strategies more efficient (e.g. through faster security information-sharing), more effective (e.g. by improving security information-gathering), visually clearer (e.g. by using advanced incident mapping tools) and more democratic (e.g. by equipping national staff members with the same security tools as international staff). In short, aid agencies have created, discovered and implemented various technological features that help them to better manage the security of their staff members.

Next to technologies that are directly incorporated in the security management of aid agencies, a variety of other technologies are used which indirectly improve the security of aid workers. Remote needs assessments, remote aid delivery and improved registration systems, for example, reduce the need for aid workers to go into a (dangerous) area for assessments, deliveries and evaluations, as these parts of the project cycle can be done from a distance. The implementation of these technologies may not always be motivated by security reasons, but since they still have beneficial effects on the security of aid workers, it is worthwhile assessing their influence.

Technologies used in security management

Information-gathering tools

A novel way of gathering security information is through using the public (e.g. beneficiaries) as a source of (security) information (i.e. crowdsourcing) (UNOCHA, 2013: 29). Crowdsourcing refers to various methods in which 'many people contribute small amounts of data to form an aggregated larger dataset' (IFRC, 2013: 170). The information is transmitted through 'texting, e-mailing, posting or tweeting short bits of information' (Ibid.), either directly to an aid agency or to a wider audience. The data includes written text, pictures, videos and checklist (Interview 28). Nowadays, crowdsourcing is often used to map and geolocate information during or immediately after crises (Meier, 2011). For instance, after the Kenyan elections in 2007, crowdsourcing was used by mapping witness reports (Ibid.) and collecting text messages on imminent violence (Musila, 2013: 46; UN, 2008: 38-41). At a smaller scale, the battle for Kirkuk was followed by simply searching in Twitter for Kirkuk and reading the Tweets that mentioned the city (Interview 8).

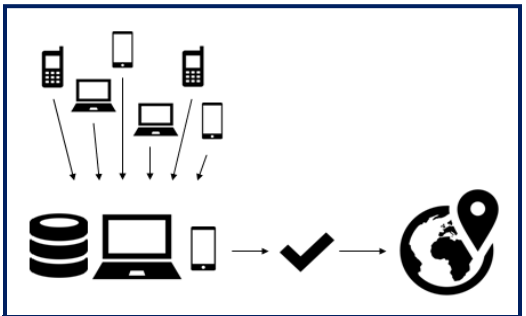

Figure 9: Crowdsourcing security information: the collection, triangulation and mapping of data received from the public or beneficiaries

Regardless of the potential of crowdsourcing, aid agencies are hesitant to trust and rely on crowdsourced data since the chance of misinformation is relatively high and a mistake can be very costly (IFRC, 2013). A related approach which tries to improve the reliability of the reported data is crowdseeding. In this approach, an aid agency selects a group of individuals, equips them with the necessary technological tools (e.g. mobile phones) and trains them in data collection and sharing (UNOCHA, 2013: 31). Since the individuals are known to the agency, agencies are more likely to trust the reported information. In addition, individuals can be trained to use codes instead of sentences in order to safeguard their security (Van de Windt and Humphreys, 2015). The *Voix de Kivus* pilot project, which used crowdseeding for gathering conflict information in Eastern Congo, is one of the first examples of this type of data collection (Ibid.).

Although the security risks assessments of aid agencies still rely mostly on the data that they (or contracted parties) collect on the ground, open sources are used more and more (Interview 12).

Local media, for instance, are consistently monitored (Interview 13)[12]. Since the immediate availability of security information is central to good security management, rapid data collection through crowdsourcing and crowdseeding can be expected to continue to expand and professionalize.

Tracking devices

Next to general information on possible threat actors, conflict dynamics and the risks that aid agencies in general face in an environment, an aid agency needs very specific security information on its own staff and assets. Since about a third of all attacks on aid workers take place while they are on the road (making it by far the most dangerous context for aid agency staff (Stoddard et al., 2014)), many aid agencies now use vehicle tracking systems (Interview 25, 27 & 29). This means that a small device in or on a car sends signals containing information on its location (and possibly other information) to a recipient. Although not at a large scale, aid workers are now even traced through their mobile phones (Interview 26 & 27).

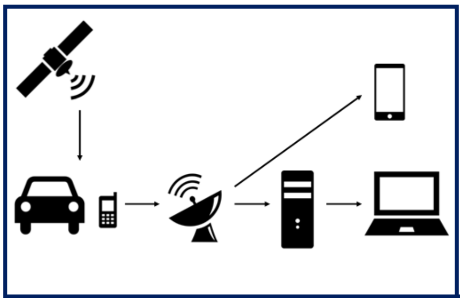

Figure 10: Tracking systems: satellite tracking of vehicles and phones

By using satellites or wireless telecommunication systems, the Global Positioning System (GPS) coordinates of equipped vehicles and mobile phones can be located, which provides the aid agency with live information on the whereabouts of its assets and staff (Ibid.; IFRC, 2013; Stoddard et al., 2014: 10). This information can be vital in the management of security incidents and can be used for the identification of the possible culprits but also for finding out which local communities can be approached to negotiate for the release of staff and which neighborhoods should be avoided during future trips.

Information-sharing tools

After security information has been collected, it needs to be disseminated in an effective and efficient manner. The use of mapping platforms proves particularly useful in this respect. Most notably, (non-profit) companies, such as Ushahidi, map and visualize crowdsourced information that assist agencies by providing up-to-date security information (UNOCHA, 2013: 31). By visualizing the (confirmed or triangulated) data over time and space, the crisis-mapping visualization enables analysis of the conflict dynamics and the risks to aid agencies (Meier, 2011). Since crises are chaotic, clearly visualized, live information as well as a thorough analysis of the conflict are essential to keep aid workers safe. Thus, crisis-mapping platforms are a valuable tool in security management.

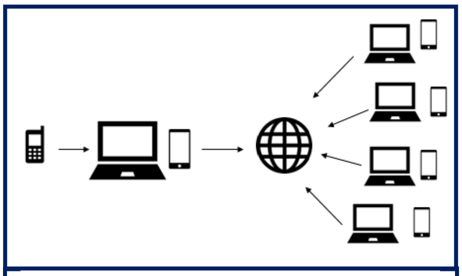

Figure 11: Electronic information-sharing: the online storage of security incidents on (mapping) platforms accessible to others

Some of the bigger agencies have begun to use their own mapping platforms as part of their security management (Interview 22 & 26). The Spanish branch of Action against Hunger (i.e. Acción contra el Hambre), for instance, uses the Ushahidi platform for incidents faced or witnessed in the field (De Palacios, 2014). By using this platform for data visualization and analysis, new risks and trends have been distinguished, which informed alternative security management measures, such as new security trainings (Ibid.)

In addition, security information is shared through new technological tools. As an example, security information-sharing between aid agencies takes place in Skype-groups (Interview 19, 21 & 24), while information is also shared through mobile phone apps (Interview 26). In addition, satellite phones can be linked to Twitter so the recipients of a message no longer have to be outside in order to

[12] Personal communication, UN official

receive the message, which makes communication much easier (Interview 5). Lastly, SMS text messages are frequently used for disseminating security information among the field staff of aid agencies (Interview 1, 24, 25 & 26). INSO, for example, sends out messages via mobile phone when a security incident has taken place (Interview 1).

Online security training

Security trainings of aid workers are an essential element of the security management approach of many aid agencies. However, a significant group of aid workers is located in areas in which it is impossible to provide training courses due to the insecurity. This is why agencies are developing online security trainings. Online training (or e-learning) 'is the use of technology for training, teaching, education and learning purposes' (Persaud, 2014: 139). Various technological tools can be used, for instance chat rooms, discussion boards, social media, Skype, blogs and e-mail (Ibid.).

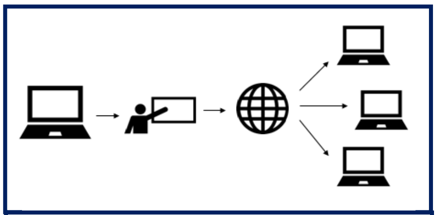

Figure 12: Online security training: the online storage of security training courses, accessible to field staff

While some bigger aid agencies developed their own online security trainings (Bollettino and Bruderlein, 2008), RedR is developing an online security training specifically focusing on local staff and local implementing partners (Interview 26). The training course exists of interactive video-scenarios, in which the user needs to make various decisions. Due to limitations in terms of finances (e.g. high production costs) and technology (e.g. fragile internet connections in the field), online security trainings are not yet able to replace face-to-face courses. Nevertheless, they can be a useful complement (Ibid.).

Technologies indirectly improving staff security

Big data: crowdsourcing and advanced computing

During a crisis, the online requests for resources by affected individuals can be used as an indication for the needs of a community. Since the number of these requests will usually be extremely high (i.e. big data) and aid delivery is hindered by a lack of up-to-date (geographical) information about the area, the help of a group of volunteers (i.e. a crowd) can play a central role in creating and processing this information (UNOCHA, 2013: 29). During the 2010 forest fires in Russia (Meier, 2011: 1248-1250) and after the 2011 earthquake in Japan (IFRC, 2013: 53-55), for instance, volunteers geolocated and mapped information about the areas and about the needs that were voiced online. Thus, next to crowdsourcing as 'using the crowd as a source of information', crowdsourcing can also refer to outsourcing some (usually technical) task to a group of people.

Crowdsourcing for aid delivery was formalized in 2010, when a group of people founded the Standby Task Force (SBTF), existing of thousand volunteers, who offered support to aid actors on translation, analysis and geolocating (UNOCHA, 2013: 29-30). Two years later, SBTF became part of the Digital Humanitarian Network, which aims to bring digital networks and professional humanitarian organizations together (Digital Humanitarian Network, 2015). Likewise, the Humanitarian OpenStreetMap Team (2015) is a team of volunteers creating free maps by using GPS, aerial images and public sources for the sole purpose of enabling humanitarian actors to do their work.

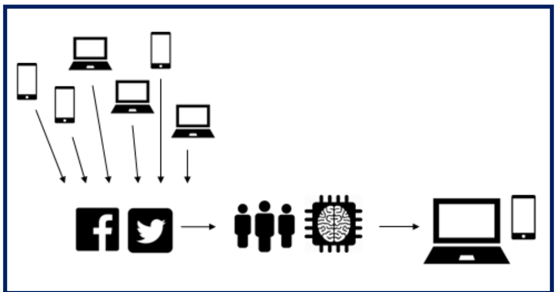

Figure 13: Big Data: the usage of crowdsourcing and advanced computing for analyzing big data

The very fact that these volunteer networks are needed, shows that aid agencies are no longer able to process the huge quantity of data on their own. Next to human computing (through volunteer networks), advanced computing systems can be used to analyze the same big data through data mining and machine learning. An example of this is SyriaTracker, a crisis map depicting human rights violations in Syria, which collects data by mining through two thousand news sources and filtering out those mentioning human rights abuses (IFRC, 2013: 91). Subsequently, information is triangulated with crowdsourced data to verify the results (Ibid.).

Social media and online news sources may be valuable sources of information, but can also be unreliable. By improving computing systems, the margin of error can be reduced. For example, on the basis of Tweet features (e.g. emoticons and word choice), classification algorithms could predict with 97 per cent accuracy whether a Tweet image of Hurricane Sandy was real or fake (Gupta et al., 2013). In a similar vein, a platform called Artificial Intelligence for Disaster Response scanned Twitter data after Hurricane Sandy. Users could identify useless or unreliable Tweets and thereby 'teach' the machine, making it more reliable (i.e. machine learning) (Ibid.: 92). Irrespective of the wide range of opportunities that this data offers, big data analysis (through crowdsourcing or computing) is not widely used in conflict settings yet. Crowdsourcing is mostly employed in response to natural disasters, while computing systems are still quite expensive. However, in the years to come, these forms of information-gathering can be expected to significantly rise in popularity and usage.

Satellite assessments

Satellites have been used for decades, but their implementation in aid delivery was scarce until a little while ago. The recent increased access to Global Positioning System (GPS) information and satellite imagery has opened up space for incorporating satellite information into aid agencies' databases. Next to being able to geographically pin-point crowdsourced data through GPS satellites, space-based data can also be used to provide spatial and geographical information about crisis areas through Geographical Information Systems (GIS) (UNOCHA, 2013: 28-29). This spatial and geographical information can be highly valuable in mapping needs and vulnerabilities as well as the monitoring of conflicts and the evaluation of projects (Ibid.: 28-29, 41; Interview 27 & 31).

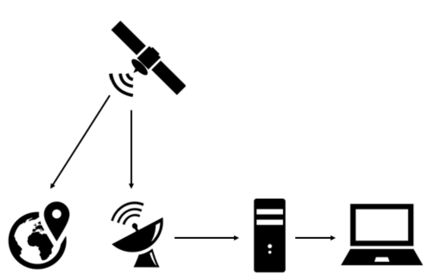

Figure 14: Satellites: field data collection by means of satellites

In addition, the Standby Task Force volunteers used satellite imagery to document informal shelters in Somalia in order to guide policy-making (Meier, 2011: 1255-1258), while the UN's Operational Satellite Applications Programme (UNOSAT) uses satellite imagery, amongst others, for human security analysis, including the documentation of violations of human rights and International Humanitarian Law (UNOSAT, 2011; Interview 8). Satellite imagery can be highly important for remote fact finding on human security issues since field access to these areas is often restricted due to insecurity, physical barriers or government unwillingness. By using satellite imagery, remnants of attacks, suspicious vehicles and damages to buildings and infrastructure can be traced, from which the size and type of an attack can be deduced (UNOSAT, 2011: 7). Satellite data is a typical example of how decreasing costs and increasing access can transform high-tech, military technologies into technologies that are useful to aid agencies.

Drones and UAVs

The use of Unmanned Aerial Vehicles (UAVs) or drones for humanitarian purposes (i.e. humanitarian drones) is recently taking off as well, as exemplified by the rising use and professionalized collaboration among current users of humanitarian drones (Meier, 2015b). Drones can (potentially) be used for data collection on a variety of issues. For instance, data of humanitarian drones can provide essential information during crises, but it can also help to document human rights violations. In addition, drones are used for improving the surveillance capabilities of UN peacekeeping missions and can deliver aid to remotely located beneficiaries (Karlsrud and Rosén, 2013; Sandvik and Lohne, 2014).

The usage of humanitarian drones is being criticized for its military connotations (i.e. the drone is a War on Terror dividend), for its infringements on privacy and for the risk of changing humanitarian action into a virtual reality (Sandvik and Lohne, 2014). Moreover, it raises the ethical concern of whether humanitarian drones should also be allowed to attack human rights violators (under the R2P framework) when witnessing grave crimes in real time (Ibid.). Apart from the many questions and critical views, drones can undoubtedly provide agencies with better and more precise information (Karlsrud and Rosén, 2013). For instance, drone images have a higher resolution than satellite imagery, which can be essential in assessing detailed needs (Interview 29), while humanitarian drones can also provide more up-to-date and precise information on refugee camps and migration flows, providing valuable input for policy decisions (Interview 27).

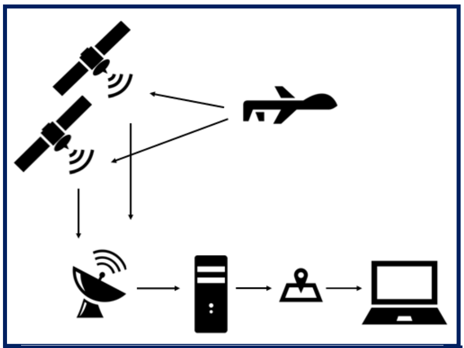

Figure 15: Drones: The gathering of geolocated aerial imagery through drones by means of communications and GPS satellites

Biometric and electronic registration

Improved biometric and electronic registration are reducing both the number of people needed in the field as well as the arbitrariness of an aid agency's deliveries, which both improve the security of the involved aid workers. Biometric registration refers to beneficiary registration on the basis of physiological characteristics. For example, UNHCR has used iris recognition tests in its repatriation program for Afghan refugees in order to be able to distinguish returnees that are entitled to assistance from those that illegally try to re-enroll and receive a second aid package (UNHCR, 2003). Elsewhere, the UN's refugee body has used fingerprints for similar purposes. The fingerprints of almost 200,000 South Sudanese refugees were collected to make aid delivery more efficient and reduce double registrations (UNHCR, 2012a). Digital fingerprinting has also been used in Senegal. The fingerprint, together with personal data, was handed over to refugees in the form of an ID card, which aimed to improve local integration and guaranteed the refugee the same rights as the native Senegalese, except for voting rights (UNHCR, 2012b).

Figure 16: Registration: biometric and electronic registration and storage of beneficiary data

Next to biometric registration, electronic registration has been subject to technological advances as well. Across different settings, aid agencies have used tablets and smart phones for conducting surveys, usually in an attempt to make the process of data collection and analysis more efficient (Interview 16 & 31; IFRC, 2013: 22-23). However, electronic registration was also used to reduce the risks of surveyors who were facing higher risks when sensitive carrying paper-forms (Interview 22). Electronic registration provides many advantages in terms of planning, monitoring and evaluating projects since everything is documented and can be easily accessed, while the chance of wrong deliveries is reduced (Interview 29).

Delivery technologies

A final set of technologies that aid agencies can use and which indirectly improve the security of their staff are technological tools for delivery. Due to security challenges, many remotely located beneficiaries are hard to reach, which is why delivery technologies that do not require aid workers to go into the field have much potential. The use of cargo-carrying drones for aid delivery is such a (hyped) example of remote aid delivery, although it is still in its infancy (Sandvik and Lohne, 2014; Interview 29).

A well-established remote delivery technology is the use of mobile cash transfers. For example, in Rwanda, a group of actors (including WFP, UNHCR, World Vision, the Bank of Kigali and VISA) came together and launched a project to provide refugees with mobile phones that were subsequently being used for monthly transactions (Tafere et al., 2014). Similarly, M-Pesa and bitcoins offer electronic money transfer possibilities. These mobile and online cash transfers are faster, more efficient and safer than the transfer of paper cash (Interview 29).

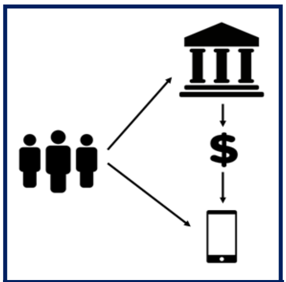

Figure 17: Delivery: beneficiaries receive frequent cash transfers on their mobile account

Security management of technologies

Challenges to the use of security-enhancing technologies in conflict settings include both electronic and physical risks, mostly related to the (electronic) collection, storage and use of data. The collection of data on beneficiaries has as a side-effect that much damage can be done if the information leaks or is stolen. Although this kind of information is not completely save in the field either, online or electronic databases can easier be multiplied and shared (Interview 29). In order to improve the information management security and prevent damage being done due to imprudent data handling, many precautionary (i.e. protection) measures can (or should) be taken by agencies operating in conflict settings (EISF, 2010).

Since data is never safe, organizations have to be very careful in their internal communication. As their communication lines may be tapped into, the information that is shared with colleagues and the phrasing of sensitive topics is also important in e-mails and phone conversations that are not meant to be read or heard by anyone else (Ibid.: 5). If a conversation is supposed to be private, (temporary) local mobile SIM cards can be acquired. To prevent tracking, the battery can be removed, since even switched off phones can reveal the location (Security Management Initiative, 2009). Public computers (in internet cafes) or public internet connections should be avoided, since these are generally conducive to abuse. Encrypted connections are preferable as well. Also, anti-virus software is essential and should be updated regularly, but free anti-software may be fraudulent which is why careful consideration is warranted (Ibid.).

Regarding their external communication, aid agencies often publish the stories and images of victims to raise awareness and funds, but since technologies allow information to travel around the world in seconds, this may potentially be very harmful to individuals that can be tracked down on the basis of this information (IFRC, 2003: 35-36). The fact that beneficiaries more and more often share data with an aid agency via social media or other platforms results in two other challenges related to data handling. Firstly, Internet Protocol (IP) addresses can be traced back to the sending actor. In case an aid actor aims on collecting highly sensitive data, it, thus, needs to consider how online informants can be protected (UNOCHA, 2013: 38-39). Secondly, new means of communication have raised expectations of aid agencies' responses to crises and disasters (Ibid.). Next to handling requests for help carefully, aid actors therefore also have to manage expectations in a responsible and careful manner (Ibid.). If not, their activities may be harmed by negative (or false) expressions of disgruntled beneficiaries or other actors which attempt to evoke anger and resentment towards the aid agency (Armstrong, 2013). Just like their implementation of many technologies, aid agencies' electronic and online protection mechanisms are still in the discovery stages.

Divergent use of technologies

The use of technologies by different aid actors

A first observation on the use of technologies by aid actors is that it is rather limited in conflict settings but increasing fast. The number of large, technologically advanced projects, such as described by UNOCHA (2013) and IFRC (2013), seems to be restricted as of yet. However, many aid agencies have introduced the first new tools and devices and plan to continue to do so. While looking at the various types of aid agencies, it becomes apparent that the ICRC and the UN may have done some large high-tech projects, but they are somewhat lagging behind in terms of implementing relatively easy technologies in the countries under study.

For instance, the UN's Food and Agricultural Organization in Somalia is reported to use satellite imagery for monitoring infrastructural interventions (Interview 31), but UN representatives in the country report very little use of even quite basic technologies (Interview 10 & 13). According to representatives, the UN uses mobile phones for monitoring purposes and introduced Video Teleconference (VTC) technology to government counterparts, reducing the number of trips (Interview 10 & 13). In an attempt to make the organization more resilient, UNDP is researching the use of solar and wind energy for charging devices but this seems not to have been implemented on the ground yet (Interview 12). Likewise, the use of basic technologies by managers of the ICRC is limited to the use of Twitter for data collection, speaking with beneficiaries over the phone and attaching GPS coordinates to pictures or cameras (Interview 2, 6 & 8). Alternative usage of technologies is reported in the literature but not by UN and ICRC interviewees in conflict areas.

Among NGOs, there is more variety of technologies being used. Many NGOs use or are about to use electronic devices (e.g. tablets and smart phones) for doing their surveys and assessments, the data of which is usually automatically downloaded (and sometimes even translated), so analyses can be carried out faster and with lower risks (Interview 1, 16, 18, 22, 28 & 31). In addition, GPS codes are often collected for geolocating needs or monitoring projects (e.g. by GPS codes on photographs or camera images) (Interview 1, 20, 29 & 31). NGOs also use mobile phones for monitoring and evaluation purposes (Interview 16 & 31) as well as advanced forms of electronic registration and data analysis (Interview 29) and BGAN or VSAT internet systems to cover failing internet connections (Interview 3, 5 & 25).

With regard to their security management, many NGOs track their vehicles through GPS tracking devices (Interview 16, 25, 26, 27 & 29). Furthermore, modern communication tools, including mobile phones, Skype and SMS alert systems, are used for security information exchange and in order to enable communication between security managers and field staff (Interview 21 & 25). NGOs are also experimenting with the use of technologies for security management. For instance, agencies design online security training courses (Interview 26), they combine old and new technologies by linking satellite phones to Twitter (Interview 5) and they are establishing online systems for sharing security incidents on a global or national level (Interview 26 & 30).

A particularly noteworthy finding in the use of technologies by NGOs was the role of donors (e.g. ECHO, USAID, DFID). Since the donors decide which projects are funded, they also have an influence on which technologies are funded. In order to minimize diversion, donors in Somalia, for instance, stimulate the development of new technologies (Interview 20). At times, donors even fund the research and development of technologies (Interview 31). Exemplary for this is the donor funding for RedR's online training course (Interview 26). In practice, it proves essential to be able to convince (especially institutional) donors of the advantages of using a new technology (Interview 29), but in general they seem have to quite positive attitudes towards using technologies in conflict settings.

The use of technologies across different settings

Although large, technologically advanced projects seem rather scarce in the countries of this study, the quite widespread use of the above mentioned technologies is striking. Not only do many technologies still come with financial challenges, but the nature of the conflicts of these countries pose an additional obstacle. For example, in Somalia and Afghanistan, the use of GPS codes and smart phones can be hindered by Al Shabaab's and the Taliban's opposition against it (Interview 1 & 31). Next, in South Sudan, mobile phone networks are often absent, while difficulties regarding permits further discourage the use of technologies (Interview 5). Lastly, the relative low education of many intended users makes implementation harder as well in countries as Somalia and South Sudan (Interview 29).

Nevertheless, aid agencies in Somalia use a broad array of technologies, varying from GPS codes on pictures and photographs to the use of mobile phones for monitoring ends (Interview 6, 10, 20 & 31). In addition, data collection software (including electronic devices) are used and will be used more frequently in the near future (Interview 18, 28 & 31). Lastly, the UN has been introducing VTC technology and satellite data collection as well in Somalia (Interview 13 & 31). In Syria, reported use of technologies includes digital Google-forms for surveying (Interview 22), Skype, mobile phones and generators or solar cells for power as well as VSAT internet systems (Interview 3). In Iraq, vehicle-tracking devices and Twitter are used in the security management systems as well, while electronic devices are an important part of the needs assessments (Interview 8 & 16).

Lastly, the reported use of technological tools is somewhat limited in Afghanistan (possibly due to Taliban opposition) and South Sudan (possibly due to government restrictions and a lack of technological infrastructure). Skype and mobile phones are used for security information exchange (Interview 21 & 25), but the use of technologies in South Sudan is otherwise limited to occasional BGAN systems for internet connection (Interview 5) and the use of electronic devices for data-gathering (Interview 29). Agencies operating in Afghanistan also collect GPS codes (Interview 1 & 2) and track their vehicles with tracking devices (Interview 25).

Technologies for security in relation to social science theory

Although technologies greatly enhance the effectiveness and efficiency of aid agencies' security management, the technologization of security management also transforms risk management into a virtual reality (Donini and Maxwell, 2013). Similar to the risk of a rising use of technologies in aid provision, this process of technologization may lead to better visibility of security risks but a social, emotional and psychological detachment of the security environment. This problem of 'cyber security management' is not easily recognizable in the field since few agencies completely rely on technological tools as of yet. The progressive rise in the use of technologies for security purposes, however, warrants caution.

Using Foucault's theory, the rising use of technologies enables senior aid agency staff, as current personifications of sovereigns, to increase the efficiency and effectiveness of their disciplinary power over their staff members. Prominent examples of this are the use of tracking devices, which enable advanced surveillance methods, and online training courses, which aim to adjust behavior through online classes. Crowdsourcing is possibly the most typical example of how agencies use the massifying mode of power. Admittedly not focusing on society as a whole, aid agencies, as new sovereigns, collect and analyze large swaths of data (e.g. on security events) in order to define general rules and guidelines for the behavior and movements of the aid agency's staff members (as a mass, rather than as individuals). The 'boomerang effect' that Foucault distinguished is applicable to our times as well. Just like the aid agencies use drones and Big Data for the control of beneficiary populations, Western sovereigns use the same tools in Western countries. Graham (2011), for example, describes how drones were used in the colonial peripheries at first, but are now also adopted in Western countries by, for instance, police forces. Thus, according to this interpretation of Foucault, the use of technologies for aid in conflict settings does, in the end, affect the lives of every human being (i.e. the entire global mass).

Many technologies are invented and developed by national militaries. Satellites, for instance, were designed for military purposes, just like internet, drones and biometric registration tools. The usage of these technologies by aid agencies leads to a militarization of aid by blurring the lines between aid actors and military actors. The usage of some of these technologies (i.e. internet and satellites) are unlikely to be witnessed by beneficiary communities that are unaware of these technologies or not using these themselves. Drones and biometric registration tools, however, are very physical and clear embodiments of the militarization of aid, leading aid agencies to either refrain from using them (Interview 2) or be cautious about their implementation (Interview 29).

While technologies in the security management of agencies aim to improve the resilience of aid agencies so they can continue to deliver their aid services, security strategies rely on continuous resilience-enhancing efforts as well (EISF, 2010). Taking a Beckian view, the process of continuous renewal and replacement of technologies in order to make agencies more resilient is symbolic for Beck's prediction that Western societies, including Western INGOs, are increasingly occupied with preventing risks (Beck, 2006). Big data software, for example, is constantly refined in order to reduce its margin of error, whereas information-sharing tools require frequent security updates as well. In turn, updates and new tools create new risks, leading to new technological feats, and thus add to a never-ending cycle of technological resilience-enhancing efforts.

The increasing use of technologies in the aid sector's risk management has diverging effects on the commercialization of aid. On the one hand, it makes aid agencies more reliant on partnerships with commercial actors who produce or develop these security tools, while technologies also enable these actors to use their 'humanitarian' collaboration with aid agencies for marketing purposes, both of which blur the lines between traditional aid agencies and companies. On the other hand, security-enhancing technologies reduce competition between aid actors as well, since it allows for better security information-sharing and communication among agencies, resulting in less commercialization and more cooperation.

Conclusion

A variety of tools are used by aid agencies which directly or indirectly improve the security of aid workers. Within the security management systems of aid agencies, new security information-gathering tools are designed whilst tracking devices are being developed. Also, security information-sharing tools and online security trainings are implemented. At the same time, various technologies are introduced in the aid sector which allow (international) staff to work from remote locations. These technologies include information-gathering and analysis tools (e.g. crowdsourcing, big data, satellite assessments and UAVs), information-storage tools (e.g. biometric and electronic registration) and delivery technologies (e.g. online cash transfers). These technologies lead to new vulnerabilities against which aid agencies have to protect themselves. While the ICRC and the UN have conducted some large-scale technological projects, the introduction of relatively basic technological tools is somewhat lagging behind in comparison with NGOs, which, sometimes encouraged by donors, make quite extensively use of technologies, especially new communication tools, GPS coding and electronic data systems. The use of technologies is somewhat limited in South Sudan and Afghanistan, but it is noteworthy that even in the most highly volatile settings in this research, technologies are being introduced and developed, even though there are serious challenges to using these technologies. Theoretically, these technologies in security management may detach aid workers from the security conditions in the field or, from a Foucauldian view, help aid agencies (as modern sovereigns) to better follow and control the aid worker masses. At the same time, these technologies, mostly with a military origin, blur the lines between aid and the military, whilst constantly requiring resilience-enhancing updates or renewals. Lastly, they may commercialize aid through increasing collaboration between aid actors and business, but these technologies also allow for better security information-sharing and communication among aid agencies, which reduces the competition among them. In short, the theoretical consequences of the technologization of risk management warrant caution, but the practical benefits are undeniable.

Chapter 6: Views on Remote Management

Views on Remote Management

Remote Management is the ultimate outcome of the use of technologies for aid delivery in conflict settings (IFRC, 2013: 137). With the help of technologies, increasingly more parts of the aid project cycle are managed from a distance. This strengthens aid agencies' protection strategies by reducing the exposure of their staff since staff members no longer have to go into the field but can manage projects remotely. For instance, 'remote needs assessments' are conducted through crowdsourcing, big data analysis, drones and satellite imagery, while 'remote security management' makes use of tracking devices, online security trainings and electronic security mapping platforms. Also, communication tools, such as mobile phones and Skype, easily and cheaply connect people in very remote locations, whereas even the registration does no longer require interaction between aid agency staff and beneficiaries because people can be registered biometrically and electronically. Although even some aid delivery is already being done remotely (e.g. online cash transfers), national staff members and local partners are still needed to provide most of the aid delivery in conflict areas.

There can be various reasons to use Remote Management. Motivations for Remote Management include infrastructural challenges (especially during the rainy season), bureaucratic obstacles (e.g. no visas granted to aid workers) (Steets et al., 2013), operational ideals (e.g. decentralization to be close to the field) (Interview 26 & 27) and financial considerations (Interview 27 & 30). However, in most cases, high or rising security risks are the (main) reasons for aid agencies to manage projects from a remote location. Since technologies enable Remote Management and these technologies can be expected to play an ever greater role in the project cycle of aid actors, Remote Management becomes increasingly more attractive and affordable. Therefore, it is useful to take a closer look at how aid agencies and critics look at Remote Management. Instead of an elaboration on the relation between Remote Management and social science theories (which will be discussed in the next chapter), this chapter interprets the views of some moral theories on Remote Management by relating the discussions on Remote Management to 'aid ethics'.

Defining and re-defining Remote Management

As mentioned before, Remote Management in this research is defined as 'a mode of operation in which international staff, either after relocation, after evacuation or by design, manages a project from a distant location because of high or increasing security risks, while national staff members or local partners implement the project on the ground'. Although this definition is different from other definitions (due to the fact that it includes projects that are managed remotely by design), it overlaps to a large extent with most existing definitions. Nevertheless, some remarks are worthwhile adding.

An often mentioned point of critique is that there is no concept covering projects that mix direct implementation (including direct expatriate supervision) with Remote Management. Quite a few security managers mentioned their hesitancy or disagreement as to whether projects (should) fall within the category of Remote Management if staff is able to visit the project regularly (Interview 6 & 20). Following OCHA's report, which coined this type of projects 'soft remote management' (Egeland et al., 2011: 26), this research includes those projects that are managed remotely but can be visited once in a while, because the management of these projects is still located in a distant place. In addition, it is of no concern whether international staff manages the project from abroad or from a safer region within the country. As long as the senior management cannot visit the field due to security reasons, the project is labeled as Remote Management (e.g. Stoddard et al., 2010).

Another aspect worth mentioning is that aid agencies can combine direct implementation and Remote Management within one country. Since it rarely happens that an entire country is too dangerous for internationals, an aid agency will usually make use of different implementation strategies within the same country (e.g. in South Sudan and Iraq). Further, national staff members or local partners sometimes distribute aid packages in areas that are considered 'no-go areas' for internationals. Due to the fact that this aid delivery requires little 'management', this type of activities has also been called remote operations (Interview 16). However, since every project requires some management (e.g. in terms of design), this research also considers these projects as a subset of Remote Management.

Hansen (2008: 5) makes a distinction between different types of, what he calls, remote programming. Firstly, there is 'remote control', which means that international managers are transferred but still take the decisions (Ibid.; Somalia NGO Consortium, 2009). A second type he distinguishes, is 'remote management', which refers to the situation in which some authority is delegated to national staff (Hansen, 2008: 5). Thirdly, 'remote support' or 'remote oversight' refers to a situation in which decision-making in the long run is left to the national staff or local organization (Ibid., Somalia NGO Consortium, 2009). Fourthly and lastly, there is 'remote partnership' referring to an equal partnership between an international aid organization and a local one (Ibid.). Although this distinction is conceptually useful, its practical relevance is compromised due to the fact that the different types are often mixed (Abild, 2010). Besides, all these different types have the same goal: providing aid without expatriate staff presence in an area where the only serious alternative is complete withdrawal (Stoddard et al., 2010). Since the reality of remotely managed project is too complex to fit within Hansen's framework, this research will use the broader umbrella term for Remote Management as defined above.

Lastly, some researches distinguish between national and local staff, with the former term referring to staff that is from the country but not from the area in which they work, while the latter term refers to people that are from the specific area (Stoddard et al., 2010: 11). In a way, Remote Management emphasizes or even creates this distinction between national and local staff. Firstly, senior national staff can be burdened with extra decision-making responsibilities, which clearly distinguishes them from local staff implementers. Secondly, senior national staff may not be from the same region in which they work, meaning that they are at a higher risk than local staff and thus more likely to be relocated (Ibid.). National staff is therefore usually part of the group of 'relocatables' (i.e. those staff members that are relocated if the situation deteriorates), while local staff are 'non-relocatables' (Interview 21). This has led some researchers to include the relocation of national staff from the field as part of Remote Management (Stoddard et al., 2010). This research, however, does not make the distinction between national and local staff for two reasons. Firstly, during the interviews, only one interviewee made the distinction (Interview 21), while most others used the terms 'national staff' and 'local staff' interchangeably. Moreover, locally hired staff usually fulfills support jobs (e.g. cooking and driving) rather than implementing jobs, which means that the relocation of national staff often means that projects practically come to an end. This research therefore only distinguishes between international and national staff. Consequently, Remote Management only refers to those modalities in which international staff members, who usually hold the management tasks, are removed from the field.

Views on Remote Management

Another programming modality

Roughly two different stances towards the practice of Remote Management can be identified. Firstly, although virtually no one is unequivocally positive, it is frequently viewed as the least unfavorable option. Taking into account that there are challenges, Remote Management also has many advantages. Firstly, local implementing partners are expected to have built-in acceptance and can keep a low profile, which reduces the overall security risks (Interview 17 & 22). Also, the collaboration with local partners fastens the response after a crisis and leads to better information (Interview 26), while their capacities are built up over the course of a project (Stoddard et al., 2010). Objectively speaking, taking risks in order to improve your home-country and help fellow citizens seems more sensible than asking or expecting foreigners to do so. When given appropriate security tools, Remote Management is therefore not an irrational strategy (Interview 30).

Next to mentioning the advantages, several aid agency representatives shared a certain passive acceptance of the strategy. Although stressing the absence of their fundamental support for the strategy, the necessity of using Remote Management was seen as undeniable in various circumstances (Interview 24 & 27). In some cases, it might be tempting to simply abandon the place, but the delivery of (life-saving) aid and the control over the risks should be balanced which might lead to the use of Remote Management as an outcome (Interview 31). While not ideal, Remote Management is therefore expected (and accepted) to be here to stay as long as NGOs seek sustainability and try to continue to operate in highly volatile environments (Interview 26).

A last resort

Secondly, another group of security managers and country directors is either outright opposed to the use of Remote Management or labels it as a 'last resort' option. Frequently, interviewees provided alternative definitions which enabled them to say that the strategy was not used by their agency, while, according to the definition in this research, a form of Remote Management was being applied. Questions on Remote Management were also regularly met with avoidance, silences and short answers , which showed the sensitivity of the topic (see Fuji, 2009). In addition, a reference to an aid agency's work as being implemented with a Remote Management strategy resulted in conceptual discussions more than once, further demonstrating its unpopularity among a group of interviewees.

Remote Management is often seen as a last resort by these interviewees because it sends the wrong message to national staff and because it makes returning to direct implementation very hard (Interview 12 & 25). Furthermore, monitoring and evaluation are compromised in remotely managed projects, leaving such a project vulnerable to corruption as well as poor implementation (Interview 13). Also, being present in the field is seen to give the aid agency more credibility and legitimacy (Interview 13 & 15). In short, 'no one is doing Remote Management by choice', but, nevertheless, it is integrated in the aid spectrum now and will continue to be used to get access in places in which this would otherwise be impossible (Interview 3).

Views of types of aid agencies compared

The views on Remote Management within the UN are diverse. One group stresses the risks in terms of corruption and fraud when expatriate staff is located far away (Interview 10 & 13). In order to have credibility and an understanding of the situation, the UN needs to be present, according to them. Another group, however, stresses that UN staff should not be unnecessarily exposed and that national staff can also be better protected in a remotely managed project than after a full evacuation (Interview 9 & 12). Since the UN has a centralized view on other security-related topics (under UNDSS), the absence of a UN-wide policy or perspective on Remote Management is striking for the sensitivity of and disagreements on the strategy.

Across different conflict settings, the ICRC is using Remote Management in various degrees and diverse ways. This may partially explained by the fact that the ICRC possibly has the widest coverage of all agencies (Interview 6). While some ICRC staff members, acknowledging its challenges, are quite accepting towards Remote Management (Interview 2 & 7), others are wary of using the definition for their modality of implementation (Interview 6). One of them, for instance, noticed that it does not matter whether staff is expatriate or national since both staff members are, first of all, ICRC staff. Admitting that the operational distance to the field increased with the departure of international staff, this manager preferred to only use the term Remote Management for projects in which non-ICRC entities are tasked with the project implementation (Interview 8).

NGOs have very diverse views. After the use of Remote Management really took off due to targeted attacks in Iraq since 2003, NGOs have used it in virtually every conflict setting to get or continue to have access (Interview 3). However, the general belief is that Remote Management will lead to deteriorating quality when it is used over an extended period of time (Interview 4). In low-risk environments, there may be many advantages (e.g. lower costs and building capabilities), but in dangerous settings, it seems to be final option, 'short of suspending operations completely' (Stoddard et al, 2010: 11). Therefore, it seems to be quietly accepted by virtually all NGOs.

An interesting finding is that headquarters' staff is less critical of Remote Management than their field-based colleagues. At the UN, for example, global security managers focus on the advantages and the necessity of Remote Management, while field security managers are more concerned with the negative effects (Interview 10, 11, 12 & 13). Similarly, ICRC staff in Geneva proves more accepting towards Remote Management than ICRC staff in Iraq and Somalia (Interview 2, 6, 7 & 8). Admittedly somewhat less obvious, global security managers of NGOs have mixed feelings and are concerned about the transfer of risks (e.g. Interview 26), but field-based staff has the tendency to formulate their concerns in stronger terms and is inclined to call it a 'last resort' (e.g. Interview 25, 26 & 27).

Views on Remote Management and the duration of use

The difference in views on Remote Management is particularly striking across different settings. Syrian aid agency security managers are least critical of the strategy as Remote Management is claimed to reduce the risks significantly (Interview 22) and projects are of a satisfactory level (Interview 7). In South Sudan, Remote Management seems to be used for a combination of infrastructural reasons and security reasons (Interview 5), leading aid agencies to be generally accepting with as main difficulty that national staff tends to lack the security resources that are provided to international staff members (Interview 21).

In Iraq, there is some more hesitancy towards Remote Management. The concept is said to be blurred and the distinction between national and international staff artificial (Interview 8), while allegedly some projects are more remote operations or remote delivery than Remote Management (Interview 16). Nevertheless, it is recognized as a necessity in high-risk areas (Interview 24). The views in Afghanistan diverge, with some mentioning the challenges but not criticizing it strongly (Interview 2), while others label Remote Management as a last resort option which will not work over a longer period of time (Interview 25).

Aid agencies operating in Somalia are almost undivided in their very cautious and critical views on Remote Management. Across institutional divisions, representatives deny the use of Remote Management, question existing definitions and criticize it for various reasons (e.g. Interview 6, 13, 14, 15 & 20). Nevertheless, especially in South Central Somalia, it seems to be the only option left to aid agencies. The critical view may partially be explained by the fact that there were some very high-profile fraud and diversion cases after aid agencies had partnered with third parties in response to the 2011 famine in Somalia (Interview 31). Ever since, many aid agencies refrain from publicly declaring or admitting their use of Remote Management.

Taking a closer look, a noteworthy pattern can be distinguished. In summary, perceptions of Remote Management are least negative in Syria and South Sudan, while aid agencies in Somalia are most disapproving. Aid agency representatives of Iraq and Afghanistan take a middle position. Strikingly, these views coincide with the temporal duration of Remote Management. As a strategy, it is quite new in Syria and South Sudan (e.g. Da Costa, 2012), while the first forms of Remote Management were already being implemented in Somalia and Afghanistan a few decades ago (Stoddard et al., 2010). Although this does not necessarily mean that there is a causal relation, it demonstrates at the very least that even after several decades, Remote Management may still not be developed in such a way that it functions satisfactorily in the eyes of senior managers.

National staff views

Since views on risk and Remote Management are intrinsically socially constructed, security managers and country directors were asked how they think their national staff perceives Remote Management. By studying the senior management's views on national staff's perceptions, the influence of those staff members that are most affected by the decision to 'go remote' could be highlighted. Stoddard et al. (2010: 24) reported earlier that national staff frequently felt resentments and an absence of the protection of their interests, while Egeland et al. (2011: 41) found that national staff thinks that their expatriate counterparts overestimate the risks.

Of the security managers that were asked questions about their national staff's views, only one security managers could refer to actual conversations that he had had with national staff on this topic (Interview 12). Because this security manager had sent security reinforcements (e.g. escorts) and continued the payment of salaries, national staff did not feel abandoned, he claimed (Ibid.). Another security manager mentioned that it is a great opportunity for a national staff member to work for an NGO (Interview 22), while others refer to the dedication of national staff to their work and their desire to continue aid delivery (Interview 7 & 11). Lastly, one (organization-wide) security manager indicated that he imagined national staff to be 'less than enthusiastic to be left behind when international staff pull out', but that that his agency is open to national staff about the possibility of Remote Management (Interview 9). In short, the influence of national staff's views on Remote Management decisions seems marginal at best.

The donor perspective

A final group that has both a strong formal and informal influence on the use of Remote Management are the donors, both institutional donors, such as USAID and DFID, and Member States (in the case of the UN). In their funding preferences, they steer policies and practices. While donors obviously prefer direct supervision (Interview 22), they seem relatively sensitive to the difficulties that aid agencies face (Interview 31). Some donors are more flexible than others (Interview 14), but generally they accept (and will have to accept) the access difficulties that some of these high-risk environments pose (Interview 17 & 18). Frequently, it is either aid provision with less control or no delivery at all (Interview 3). Although donor pressures are being felt towards the reduction of costs and the continued presence of internationals, they usually have a hands-off approach on Remote Management, because aid agencies are believed to have a better grasp of the field and in order to reduce the risk of liability in case something goes wrong (Stoddard et al., 2010: 33).

It is difficult to distinguish between donors' willingness to fund Remote Management, since representatives were not very outspoken on this issue. Looking at their publications, ECHO seems a bit more hesitant, stating in a 2013 report that it will not fund projects 'using remote management, other than in the most exceptional circumstances' (ECHO, 2013: 2), after which it lists a long set of strict criteria to be fulfilled before Remote Management is allowed as an implementing modality. DFID, on the other hand, seems more willing to support these projects. It generously funds a broad variety of remotely managed humanitarian and development activities (DFID, 2015). In conclusion, donors are critical but open to supporting Remote Management.

Remote Management and ethics

Throughout this research, the practice of Remote Management evoked moral questions and criticisms. Remote Management is seen as a strategy in which risks are transferred from the expatriate staff onto national staff or local partners (Interview 26). They are expected to become more vulnerable when internationals leave, while already receiving fewer security resources (Donini and Maxwell, 2013). This 'risk transfer' is criticized by many interviewees and experts. Since the moral question surrounding Remote Management affect the views on the strategy significantly, it is worth studying it in some more detail. Two questions are to be answered. Firstly, is there a transfer of risk from expatriate staff to national staff in Remote Management? Secondly, if this transfer of risk does take place, is it morally questionable or objectionable?

Transferring risks

Interestingly, the literature assumes rather than proves that a transfer of risk takes place in remotely managed projects, so many sources leave the claim unsubstantiated (e.g. ECHO, 2013; Hansen, 2008). One of the practical examples of a risk transfer refers to a case in Somalia, in which national staff faced higher risks because they were seen as the new decision-makers (Interview 4). However, since a fundamental study of the link between Remote Management and risk transfers is absent, this incidental evidence cannot be extrapolated to all remotely managed projects .

Most reports therefore refer to expectations rather than proven correlations. For instance, in a chapter uncomfortably combining ethical and liability issues, Stoddard et al. (2010: 27) mention that malicious actors *may* target national staff when their international counterparts are withdrawn in order to drive out the agency entirely or because they are the 'next most valuable target'. Donini and Maxwell (2013) highlight that national staff and partners face pressures that internationals would not face, but they fail to elaborate which pressures are meant. Egeland et al. (2011: 25), stating that national staff from different regions may be distrusted as much as international staff, overlook that this risk will be present for these staff members, irrespective of the use of Remote Management.

A second point of concern in this discussion relates to the term 'transfer'. When arguing that Remote Management leads to a transfer of risks from one group to another, this supposes that the risks that were originally faced by international staff are now threatening national staff. This assumption is questionable. National staff faces very different risks than international staff (e.g. ethnic rather than anti-Western), which means that the term of risk transfer oversimplifies reality. Also, some risks are unlikely to be transferred (e.g. the risk of car-jacking when only internationals drive cars). Lastly, the literature ignores the potential risk reductions for national staff in remotely managed projects (e.g. it is much easier to keep a low profile without expatriate staff presence). In brief, although it may be the case that risks for national staff rise due to the withdrawal of international staff, it is important to stress that, firstly, there is no substantive evidence for this claim as of yet, secondly, it is unlikely to be the case in every project and, thirdly, the term 'risk transfer' is a poor description of the situation.

Moral considerations

Assuming, as regularly occurs, that risks to national staff do rise as a consequence of the decision to use Remote Management, the question arises: is this morally objectionable? This question is part of 'aid ethics' (i.e. moral debates on aid-related questions). In practice, aid agencies are increasingly concerned with staff care and the moral question of risks to aid workers (see Porter and Emmens, 2009). Since national staff in remotely managed operations may face higher risks due to the withdrawal or absence of internationals, the current focus of aid agencies in terms of moral debates rests specifically upon the aid agencies' duty of care towards national staff. As one interviewee noted: '[I]n the last few years, there has been a lot of emphasis on the duty of care, on the responsibility we have for national staff' (Interview 11). In order to be able to answer the question whether heightened risks to national staff in remotely managed operations are morally acceptable, various philosophical schools of thought can be applied to the debate. In the following sections, the views of two main moral philosophies, namely deontology and utilitarianism, will be used to scrutinize the morality of Remote Management if it leads to higher risks for national staff.

Immanuel Kant, the father of deontology, argued that an action is moral if you can rationally want the maxim of the action to be universal (i.e. hold under all circumstances) (Kant, 2004). For instance, one needs to speak the truth, because it is rationally preferable if everyone always speaks the truth (i.e. the maxim of speaking the truth can be universalized). When applying this theory to Remote Management, identifying the maxim is more challenging. Following Kant's line of thought, the maxim could be formulated as: 'The risks that an individual faces can be re-ordered, if this reduces the overall risk to the group of individuals'. This maxim, however, would not receive Kant's support for it cannot reasonably be universalized. For instance, if person X makes a mistake, which leads to a risk to both person X and (the less vulnerable) person Y, it is unreasonable to shift the entire risk to person Y with as motivation that this would reduce the overall potential effects of this risk. In other words, this maxim would take away personal responsibility, which is an essential element of Kant's moral theory (Ibid.). On the other hand, if a project is remotely managed by design and a national staff member would choose to participate (assuming there are no perverse incentives to do so), Kant would most likely not object, since morality demands free choice of every individual.

Utilitarianism, as a consequentialist moral theory, focuses on outcomes, rather than motives or maxims (Rachels and Rachels, 2009). With regard to its view on Remote Management, the utilitarian ideal of maximizing the happiness of everyone involved, is the guiding principle. If expatriate staff faces higher attack rates, Remote Management reduces the overall suffering of aid workers, because the rise of attacks on national aid workers, if present, does not weigh up against the reduction of attacks on international aid workers (or the strategy fails to reach its goals altogether). However, a complicating factors is that beneficiaries may face deteriorating quality of projects, which limits the overall happiness caused by Remote Management. In brief, there is no easy calculation that can clearly tell whether utilitarians would be in favor or opposed to Remote Management. Contextual, background information is needed to judge on a case-to-case basis whether Remote Management reduces the overall risks to all people involved and to what extent program quality is compromised in order to decide whether Remote Management is moral. In extremely volatile countries, such as Somalia and Syria, it can be expected that many internationals would suffer from attacks, while the added benefit of their presence is probably marginal, leaving Remote Management as the morally preferable implementing modality, but in other areas, resorting to Remote Management is likely to be morally more ambiguous.

The ethics of Remote Management reconsidered

There is no clear answer to the question on the morality of Remote Management. Common belief has it that Remote Management faces many ethical questions due to its transfer of risk from international staff to national staff. However, a brief study into the questions whether there is a transfer of risk to national staff and whether this transfer of risk is morally objectionable, offers some nuance to the debate. The transfer of risk seems to be a poorly chosen term, while there is no substantiated research on the rise of risks for nationals in Remote Management and this is unlikely to always be the case. With regard to the question whether this rise of risks for nationals would be immoral, it can be argued that it only is immoral if the project shifted to Remote Management instead of being designed as such (Kant's deontology) or that it depends on the contextual background but that, in dangerous settings, it is likely to be morally justifiable (utilitarianism).

Conclusion

Since the concept of Remote Management is contentious, every definition is bound to be criticized. As opposed to existing definitions, the definition in this research includes projects that are occasionally visited by expatriate staff but managed remotely and projects that are remotely managed by design, which broadens the scope to encompass more projects than other definitions. The views on Remote Management by security managers and country directors vary from labeling it as 'another program modality' with its own specific disadvantages to a 'last resort' option. Within aid agencies, there is disagreement on the merits of Remote Management. Strikingly, headquarters' staff is inclined to voice a neutral view, while field-based staff tends to be more critical. In addition, in countries with a long history of Remote Management (e.g. Afghanistan and Somalia), aid agencies are less favorably disposed to Remote Management, whereas aid workers are more positive in countries in which Remote Management is a fairly recent phenomenon (e.g. South Sudan and Syria). A point of concern is that aid agency managers are relatively unaware of (and seem to give little weight to) the views of their national staff on Remote Management. Donor views, however, are perceived to be quite open and flexible, with minor variations among donors. Lastly, the common belief that Remote Management leads to a transfer of risks onto national staff and is therefore morally ambiguous can be challenged by arguing that the term 'risk transfer' is not a flawless description of reality (since risks are not so much transferred but rather altered due to Remote Management), while, depending on the moral theory, the morality of changing risk profiles in Remote Management is not necessarily morally objectionable either.

Chapter 7: Implementing Remote Management

Implementing Remote Management

Virtually all aid agencies that were interviewed for this research used a form of Remote Management. While Remote Management was the main or even only implementation modality for some, others used it rather sparsely for a specific geographical area or for a limited number of time. Although the strategy is being used by virtually every aid agency in the countries included in this study, interviewees did not refrain from criticizing its disadvantages and sharing the difficulties of managing a program remotely. Various inventive steps have been taken to deal with these challenges, while taking into account the context and its limits.

Contextual factors have resulted in very different implementation structures of Remote Management. For instance, the security situation in an environment determines whether international staff is able to visit project sites that are managed from a distance. Similarly, depending on the maturity of the civil society, aid agencies can choose to partner with a local NGO or opt for hiring its own national staff to implement remotely managed projects. Also, as Hansen (2008) mentions, based on the aid agency's preference, it can transfer different degrees of responsibility and decision-making power to its national staff or national counterpart.

The main means to work around the challenges to Remote Management is by making use of new technologies. As one interviewee put it: 'Remote Management is not a big deal if you have access to technology' (Interview 3). Historically, Remote Management faces serious difficulties with regard to planning, communication among staff, the security of implementers and quality monitoring. By using technologies that were identified earlier, aid agencies are now increasingly able to reduce these challenges of Remote Management.

Variants of Remote Management

Main categories

In this research, Remote Management through national staff was the most frequently identified Remote Management modality. Regardless of the country or type of aid agency, national staff is implementing projects on the ground while receiving directions and being supervised by international staff that was either in a safer area of the country (e.g. Iraqi Kurdistan or Juba) or abroad (e.g. southern Turkey or Nairobi). If at all, visits from expatriate staff usually takes place every fortnight (e.g. Interview 14) or every month (e.g. Interview 18).

The second most popular form of Remote Management exists of partnering with a national NGO and supporting this organization in the implementation of the project that is designed by the INGO. This strategy is especially useful for building ties with a community in areas in which the aid agency has not worked previously or in order to support capacity-building of the local NGO (e.g. Interview 17). Next to simply using national staff and national partners, variants of Remote Management have been developed. These variants are worth mentioning since they will most likely be used again or further developed in the near future.

Alternative structures

One way of implementing a project without direct field access or supervision from internationals is contracting a (for profit) third party. In Iraq and Syria, for example, water-related projects are implemented by local contractors (i.e. water engineers), with which agencies have worked previously. After finishing their job, these contractors are asked to document their activities and make pictures of their work for monitoring purposes (Interview 7 & 8).

One agency closely collaborates with the local communities in which it is implementing a community development project. In these villages, committees are founded that have to meet a range of criteria (e.g. inclusion of women). Several activities are carried out by visiting national staff, such as elections and surveys, but the village committee has the final responsibility. When the committee members are elected and trained, the village receives a grant which it may spend according to its own preferences. The execution of the chosen project is supported by the INGO. In this variant of Remote Management, the village committees are strongly involved in the project evaluation (Interview 1).

Some aid agencies partner up with government bodies instead of communities. The development programme of the UN, for instance, assists in organizing elections and establishing a rule of law. As a consequence, its national partner is the federal government. Due to security conditions, it may be difficult to 'visit the field' (e.g. a ministry), which is why modern communication tools are frequently used instead (Interview, 13).

One agency combined the use of its own national staff and an implementing partner in one project (i.e. fifty per cent balance). Both parties to the collaboration benefit from the partnership in different ways. Whereas the INGO helps the national partner in becoming sustainable by providing support in terms of knowledge, resources and capacities, the national implementing partner helps the INGO by sharing its understanding of local politics and community issues. Also, during the project, the INGO's national staff can build up the agency's own presence and acceptance in the area and, in the meanwhile, keep oversight over the project (Interview 17).

In a similar vein, the ICRC sometimes uses its national counterpart, the national Red Cross or Red Crescent society, to implement projects on its behalf. With regard to the division of tasks, the ICRC provides the funding or resources, while the national society is tasked with distributing the goods or implementing the project. The design of the project and the logistics are worked out in close collaboration (Interview 2). The national Red Crescent societies may also occasionally carry out activities for other aid agencies (i.e. UN and NGOs), although this compromises their security (Ibid.).

Implementation differences

Implementation differences per country

In Afghanistan, aid agencies use various versions of Remote Management. The contingency plans of one INGO, for instance, show that a national staff Senior Management Team takes over in case of expatriate staff evacuation[13]. This team of national staff is to be guided in its activities by the international staff in an adjacent country (Interview 25). Another INGO supports the community in implementing its own project. In this project, national staff is tasked with conducting monitoring activities in the field (Interview 1). A third aid agency has a significant number of international support staff based in Dushanbe, Tajikistan, but its remaining international staff can still visit the main offices (Interview 2). In the rural areas, lastly, various variants are being used, including working through national staff, hiring consultants and training nationals.

Remote Management in South Sudan exists mostly of projects in which an aid agency's national staff continues operating after internationals have left. It happens quite often, for instance, that fighting is looming in an area and expatriate staff is evacuated before airfields are effectively closed down (because of a lack of a flight safety assurance), so that nationals operate without direct international supervision (Interview 21). One INGO reported that Remote Management is used as well during temporary projects in very remote locations. In those cases, national staff is tasked with the implementation and monitoring of the project, while locals might be temporarily hired as porters or laborers (Interview 5). Another agency shared that, rather than evacuating internationals, it preferred to scale down the number of staff members in an area down to one person, just to keep some representation (Interview 19). Although there are quite a lot of national NGOs in South Sudan as well (Interview 21), only one of the interviewees reported a collaboration with them but added that this was only for implementation reasons (Interview 5).

[13] This system is similar to the Shura-council system that Tearfund adopted in Afghanistan, in which five senior national staff members discuss on matters of accountability and decision-making while internationals supervise from abroad (Stoddard et al., 2010).

Agencies operating in Iraq work more often with local partners than in other conflict areas. The use of implementing partners is popular because it is easier to justify this type of Remote Management to donors (e.g. by referring to its capacity-building effect) (Interview 3). One INGO, for example, uses an experienced national NGO to provide small-scale distributions in an insecure area (Interview 24). National partners also provide deliveries in areas that are under siege or where terrorist threats of ISIL are high (Interview 16). Infrequently, there are projects in which national staff works without expatriate staff supervision (Interview 9 & 12) or where third parties are contracted (Interview 8).

In Syria, aid agencies use a mixture of various types of Remote Management, which is claimed to be the dominant form of aid delivery in the country (Howe et al., 2015). Aid agencies align with local NGOs that implement their projects on the ground (Interview 3 & 7), but they also subcontract third parties (e.g. water engineers) (Interview 7). In addition, aid agencies have national staff that implements projects without direct international supervision (Interview 11). It is worthwhile mentioning that most aid agencies work from Turkey. Before NGOs got their registration in (and access to) Turkey, some aid agencies were managing the Syrian intervention from southern Turkey while managing the Turkey office (run by nationals at that time) from Amman. This was labeled as 'Remote Remote Management' (Interview 22).

Lastly, in Somalia, Remote Management is omnipresent and some form of it is used by virtually every agency. It is noteworthy that, with the exception of one INGO, all aid agencies have either their headquarters or their support staff located in Nairobi, Kenya. While most aid agencies use national staff for the implementation of these projects (e.g. Interview 6, 14 & 15), national implementing partners are also occasionally used as they are better able to reach the most difficult locations (Interview 10). Somewhat less frequently, aid agencies have either come up with inventive alternatives, such as projects combining national staff and a national partner (Interview 17), or they work through or with government structures (Interview 13 & 28).

The question arises how these different implementation modalities of Remote Management in various countries can be explained. Firstly, it is noteworthy that the most innovative uses of Remote Management are to be found in the two countries in which the practice has existed longest, Somalia (e.g. fifty per cent balance) and Afghanistan (e.g. community implementation). This may partially be explained by the dissatisfaction about the strategy in these countries in the first place, which may have led to the search for better variants. Secondly, the limited use of local partners in South Sudan and Somalia can be explained by the fact that South Sudanese NGOs are still in their infancy, while aid agencies operating in Somalia have had some negative experiences with national partners. The popularity of the use of national NGOs in Iraq, in turn, can be explained by the long-term relative stability of Iraqi Kurdistan, which allowed for the growth of relations between international aid agencies and national NGOs. Lastly, the instability in Syria and Somalia has resulted to a more widespread use of Remote Management in these countries and the evacuation of headquarters abroad to, respectively, southern Turkey and Nairobi.

Implementation differences among aid actors

An interesting finding is that all UN security managers only mentioned the use of their own staff for Remote Management (although WFP is known for occasionally using private contractors) (Stoddard et al., 2010)). When internationals are withdrawn from the field (after a thorough risk assessment), nationals often work from home (e.g. in Kabul), although they may also be asked to look after the facilities and maintain contact with interlocutors (Interview 9 & 12). Infrequently, UN national staff is relocated or even evacuated (Interview 12). The duty of care towards national staff is now more emphasized than ever before, which has led to the (continued) provision of security and financial resources to national staff in remotely managed project (Interview 11 & 12). Support staff is located as much as possible out of a country if risks are high. For instance, the support staff of Iraq and Afghanistan is located in Kuwait, orientation trainings for Somalia-based staff take place in Entebbe and security trainings for Iraq-based staff are taught in Amman (Interview 11).

The ICRC uses the full range of Remote Management variants. In relief operations, the ICRC works through its national field officers (Interview 6), who can ask for a suspension of activities if they deem the risks of working too high (Interview 8). The ICRC also hires local contractors for water-related activities (i.e. water engineers) (Interview 7 & 8). Next, the ICRC implements through its national counterpart, the national (Red Crescent) society, to deliver assistance in volatile areas (Ibid.). Lastly, there are trainings of nationals in order to teach them, for example, how to fix hand pumps or provide first aid, after which they provide the aid to their own communities. The monitoring, then, is done by community elders and consultants (Interview 2).

The use of Remote Management among NGOs is, again, very diverse. NGOs use virtually all possible variants of Remote Management, including Remote Management through national staff (e.g. Interview 14 & 21) and through national partners (e.g. Interview 16 & 24). It is worthwhile mentioning that NGOs are also the most inventive in creating and developing alternative implementation structures of Remote Management (e.g. the earlier mentioned 'fifty per cent balance' and 'community implementation'). In addition, an NGO in South Sudan scales down the number of staff members to keep a minimal presence (e.g. Interview 19), while an NGO in Syria hires its local staff as contractors to reduce the risk of being affiliated with the INGO (Interview 22). There is no indication, however, that the size of the NGO, its mandate or its ideology affects the type of Remote Management that it uses. Except for Somalia and Syria, remotely managed activities of NGOs are usually of a small scale and focus on deliveries (e.g. food, NFIs, medicine) rather than services.

Implementation of Remote Management and the use of technologies

Planning

In 2010, Stoddard et al., (2010: 19) reported that Remote Management was still a reactive decision to incidents rather than a planned strategy. However, they already noticed a growing tendency among agencies to make guidelines for Remote Management which indicated a positive trend (see Interview 15)[14]. With regard to planning, several lessons have been learned. Firstly, it is widely believed that Remote Management can only be successful if the agency has had previous relations with a community or national partner (e.g. Interview 4 & 31). New projects in a Remote Management modus are doomed to fail. Secondly, some activities are better implemented under this modality than other projects. For example, easily measurable programs and item deliveries have a higher chance of success than programmes or projects that require high skills (Stoddard et al., 2010; Interview 31). In any case, an appropriate program depends on solid needs assessments, for which technologies (e.g. satellites and electronic registration) are essential. Thirdly, although Remote Management requires a lot of time, effort and planning, there is also a risk to taking too much time for preparation, as an intervention may come too late or become redundant (Interview 2).

Increasingly more projects are designed to be implemented through a Remote Management strategy, which has led some commentators to ask the question whether Remote Management has become the 'new normal' (Donini and Maxwell, 2013). The challenges of going back from Remote Management are twofold. Firstly, there tends to be a loss of contact with important gatekeepers after going remote, although these contacts can nowadays be better maintained through online communication tools. Secondly, much more information is required for going back into an area than for withdrawing, a challenge which is known as the 'Remote Management trap' (Interview 9). In Somalia and Syria, security managers and country directors did indeed suggest that it is unlikely that their agency will switch to direct implementation with expatriate staff anytime soon. This is particularly worrying since Remote Management is argued to face the law of diminishing returns (i.e. for each consecutive period of time, the benefits reduce) (Donini and Maxwell, 2013).

[14] INGO Evacuation/Contingency Plan

One of the main concerns in planning Remote Management is the lack of capacity of the implementers (Norman, 2012). In order to pick the right national partner, extensive information-gathering usually precedes this decision. In this phase, information is collected from other aid agencies (that previously worked with the national partner), government databases and open sources (e.g. social media) (EISF, 2012; Interview 18). In some settings, for instance in Syria, many potential partners are not registered and are very new, which is why Diaspora organizations may be a preferable option, although they tend to lack credibility in the country of operations (Howe et al., 2015). Finding skilled national staff can be hard as well, especially in Somalia (Interview 4 & 20). One interviewee mentioned that he had been told that 'any Somali who is educated and honest, is either out of the country or dead' (Interview 4). Although Diaspora returnees are well-educated and have good intentions, they are concentrated in the urban areas, leaving a lack of skilled staff in the rural areas (Ibid.). Agencies that are more likely to be targeted, face even bigger challenges in this regard (Interview 13). In order to deal with lacking capacities, frequent (online) trainings of local partners (Interview 1 & 24) and staff (Interview 11; Belliveau, 2013) are part of aid agencies' activities.

Finally, planning also includes the preparedness of aid agencies for possible adverse developments in their security environment. In order to enable its continuing presence in a volatile area, an aid agency therefore needs to enhance its resilience. The most prominent way to boost organizational resilience is by adopting technologies, such as sun or wind energy for power, BGAN and VSAT networks for internet connection or online cash transfers when paying out salaries in paper cash becomes too dangerous (Interview 12). As one security manager phrased it: 'Resilience is like a Swiss clock: if it gets a shock, it still keeps on ticking' (Ibid.).

Communication

Communication is the first casualty of Remote Management. Since expatriate staff is located in a remote location, contact between internationals and nationals faces the risk of being reduced in terms of quantity and quality. Direct interactions and group meetings can be very valuable in passing on technical information, sharing experiences or coming up with new ideas (Donini and Maxwell, 2013: 404). However, communication is increasingly digitalized, with the most important means of communication between expatriate staff and national staff or national partners being conversations via email, telephone and Skype (Interview 3 & 22; Belliveau, 2013; Norman, 2012).

In addition, the interaction between expatriate (decision-making) staff and the populations they serve, is believed to significantly reduce. Donini and Maxwell (2013: 408) write that, in their experience, there is 'a relationship between physical presence and contact with populations and authorities'. As aid agencies reduce their field presence to short visits, the loss of interaction harms their understanding of the field (Stoddard et al., 2010) as well as the 'acceptance' strategy which most aid agencies pursue (Donini and Maxwell, 2013). As one interviewee put it: 'the higher you build your wall, the more you are separating yourself from the community' (Interview 4). Although frequent field visits were referred to as evidence that a project should not be considered as remotely managed, Norman (2012: 15) reports that even expatriate staff members of an NGO who visited their remotely managed project twice a week were criticized by the community for not being enough in their midst. A clear and convincing communication strategy, which explains the rationale of Remote Management, may soften the adverse effects (Interview 12), but if this chance is missed, the negative effects of remotely managed projects on acceptance-building measures and the loss of understanding of the field conditions will most likely extend the use of Remote Management.

On a somewhat more positive note, communication is now more likely to be possible and fruitful in Remote Management. In 2003, for instance, when many aid agencies withdrew their staff from Iraq, communication problems were much more serious, since mobile phones and internet were not as advanced and easily accessible as now (Interview 3). Even in Syria, after years of destruction, there are generators and solar cells which provide power and there is either internet connection or there are systems which enable staff to access the internet. In addition, mobile phones and Skype can put national staff in touch with their international counterparts instantaneously (Ibid.). In short, modern communication means significantly reduce the adverse effects of not being physically in the field.

Security of national staff and partners

As mentioned earlier, the idea behind Remote Management is that nationals (both staff and partners) are at a lower risk because they know the environment (Interview 23), have built-in acceptance and can keep a low profile (Interview 17). While Remote Management, as a protection strategy, undoubtedly improves the security of international staff, aid agencies seem to be struggling with the security of national staff and implementing partners.

On the one hand, security managers mention that there is an (increasing) recognition of the duty of care towards national staff (Interview 9 & 11). When internationals are withdrawn, national staff can, for instance, work from home if the situation requires it[15]. In a few exceptional cases, national staff members has also been left with armoured vehicles or have even been evacuated (Interview 12). On the other hand, there is also a dominant belief that nationals, just because they have been in the conflict area for so long, 'know better' and need little preparation (Interview 3). It is noteworthy that many technologies incorporated in aid agencies' security management strategies (e.g. vehicle tracking) are limited to usage by expatriate staff. Although online trainings are being designed for nationals (Interview 26) and national staff has been equipped with mobile phones in order to keep them updated about security developments (Interview 25), it is unlikely that nationals are enabled with the same range of security tools as internationals (Interview 21), a situation which reminds of Beck's (1992) claim that (relative) poverty and risks attract each other. A complicating factor to the provision of security to nationals is that they may face risks that are unrelated to their work for the agency (e.g. personal disputes) (Interview 5). This problem can be tackled by only claiming responsibility for national staff members' security from the office to their home door (Interview 28).

In general, aid agencies do not express a strong sense of responsibility regarding the security of their national implementing partners. In theory, they have no other obligation than a moral one for the security of these partners (Interview 3). Also, the reason why they use national partners in the first place is because national partners can deliver where they, for security reasons, cannot deliver. Nevertheless, there is collaboration between the international NGOs and their national implementing partners (EISF, 2012: 23-29). Although INGOs are willing to invest in trainings of national partners and in exchanging information through Skype and mobile phones or by e-mail (Interview 22 & 23), the support for national NGOs remains short of the level of security support for their national staff (Stoddard et al., 2010: 25-26).

Quality and monitoring

The most serious concern related to Remote Management is its negative effects on the quality of the programs. Bad quality projects are not only a waste of resources, but can also turn the public perception against an organization (Interview 8). This is why monitoring and evaluation (M&E) is becoming increasingly important, albeit being in contrast with the rise of Remote Management (Interview 3). To keep up high levels of quality in these projects, aid agencies have developed a multitude of M&E mechanisms (Interview 23 & 25; Souness, 2011). Nevertheless, it is inevitable that the aid delivery in Remote Management will not precisely reach the intended beneficiaries. As long as the percentage of wrong delivery is small, this is a sacrifice that is accepted (Interview 2).

Of course, expatriate staff field visits are being conducted on a frequent basis as a means to improve the oversight and control (Interview 7, 14 & 15). Recently, third party monitoring has become an increasingly popular monitoring tool as well. Third party monitoring refers to the outsourcing of monitoring to, for instance, civil society, academia, private firms or consultants (DFID, 2015; Howe et al., 2015; Interview 6, 17, 23 & 31). In addition, aid agencies reported the practice of supported

[15] INGO Evacuation/Contingency Plan

supervision (i.e. collaborative supervision to identify points of improvement) (Interview 18) as well as the structural inclusion of checks and balances between different departments (Belliveau; 2013; Interview 6). Lastly, aid agencies have begun to collaborate on M&E by monitoring each other (i.e. peer-to-peer monitoring) (Interview 22 & 23).

On a rather basic technological level, beneficiaries are being called (Interview 8, 10 & 16; Souness, 2011), while GPS codes are used to track project achievements via satellites (Interview 1). Strong communication means with the field team are another way to reduce the likelihood of fraud (Interview 15). These communication means can also be used for sharing footage (e.g. live demonstrations of the project achievements via Skype) (Donini and Maxwell, 2013). Next, the IFRC (2013: 122-123) refers to an agency that combined electronic data collection and GPS mapping in a commodity tracking system, so it could follow its health items, while Howe et al. (2015) mention the possibility of community-based monitoring through crowdsourcing.

In practice, as the examples above prove, most agencies put serious thought and resources in M&E to ensure high quality projects and to reduce the possibility of diversion. Admittedly, some even go to such great lengths that their monitoring and evaluation suggest a distrust of the field (e.g. Belliveau, 2013; Howe et al., 2015). However, due to the risks of bad quality programs, the negative publicity caused by cases of fraud and due to donor requirements, M&E will most likely become more and more important in the upcoming years. Technological tools, enabling improved M&E practices, will therefore most likely become increasingly important in aid agency's operations as well.

Remote Management and social science theories

With regard to the politicization of aid, Remote Management can be expected to further contribute to the view of aid as a political means in the hands of fundamentally Western actors. Remote Management demonstrates a symbolic transfer of power from the local field offices to the Western hotspots in the region in which the expatriate staff resides (e.g. Nairobi and Turkey). In this way, the decision-making (and biopolitical) power over the field is centralized in Western enclaves, in which one can also find Western embassies and regional headquarters of international organizations. The process of centralizing decision-making in Western centers of power is likely to encourage the perception of aid agencies as fundamentally Western and political actors.

Taking a Beckian (1992) view on Remote Management, it can be seen as a stereo-typical example of the aid sector's inclination to prevent and minimize risks by avoiding dangerous areas. On the other hand, the reduced quality and monitoring capabilities that are inevitable in remotely managed projects create new risks since failing aid interventions may increase the risks of violence or disturbances. In short, Remote Management, in this interpretation of Beck, is a balancing act, weighing the risks of presence (in terms of security) against the risks of distance (in terms of project quality) in order to minimize the overall risks to modernization processes. In any case, Remote Management goes against Duffield's (2012) post-modern view on the aid sector as increasingly internalizing risks.

Remote Management can, in a certain way, be interpreted from a perspective on aid as progressively commercializing as well. The motivation to avoid dangerous areas is not only based on the fact that there are higher risks to staff members but also on the desire to mitigate liability and reputation risks (see Donini and Maxwell, 2013). The victimization of an international staff member is likely to come with compensation claims and reputation damage, terms which are reminiscent of the for profit industry. Albeit not leading to a more commercial aid industry, Remote Management does indeed seem to result from it.

Lastly, Remote Management detaches expatriate staff from the field. Proponents of basing international staff in Mogadishu frequently mentioned that being located in Nairobi would mean a loss of credibility in and understanding of the field (e.g. Interview 15). The fact that very few interviewees met their beneficiaries on a regular basis anyway is a serious point of concern in this regard. Strikingly, in the thirty-one interviews conducted (with over twenty hours of material), there was also not a single reference to human suffering or empathetic sentiments. Rather, the emotional and psychological detachment from the field was recognizable in the neutral (as opposed to personal and human) answers to questions on the activities of the aid agencies and their relations with beneficiaries and the field. On the other hand, the absence of an expression of empathy towards beneficiaries can also be explained by the fact that no questions were asked on this point specifically, which may have rendered such comments seemingly socially undesirable or irrelevant to the interviewees. In addition, security managers and country directors were asked about their professional opinions and experiences rather than their personal motivations, which, again, may have reduced their willingness or urge to express subjective sentiments.

Conclusion

Remote Management is used in all of the conflict settings studied in this research. In fact, almost every agency uses some form of Remote Management. The two dominant strands of the strategy include working through national staff and working through national partners, but there are various alternatives. The duration of the use of Remote Management spurs the creativity regarding these implementation variants. The UN (with the exception of the WFP) is solely working through its national staff, but the ICRC and NGOs make use of the entire range of implementation possibilities. The growing use of technologies reduce the adverse effects of Remote Management. On the issue of planning, technologies enable improvements in preparedness, choice of implementers and resilience, although returning remains a sore point. In communication, technologies diminish the negative influence on contact between expatriate staff and implementers as well as between internationals and the field. With regard to the security of implementers, aid agencies are lingering between an increasing sense of duty of care (and transfer of technological tools) towards nationals and the idea that national staff members are at a lower risk and know how to manage security risks themselves. Whereas there is some willingness to invest in the security of national partners as well, a sense of moral obligation is lagging behind in this regard. Lastly, with the exception of some aid delivery projects, aid agencies are seriously concerned with providing high-quality aid, which has resulted in a wide range of (mostly technologically advanced) monitoring and evaluation tools. Using social science frameworks, Remote Management can be seen as a contributing factor to the politicization of aid by centralizing decision-making in Western centers of power (e.g. Nairobi), whereas aid agencies, from a Beckian view, constantly need to balance the risks of presence (i.e. physical dangers) against the risk of distance (i.e. quality deterioration) in order to minimize the overall risks to modernization processes. When using the perspective on aid as increasingly commercializing, Remote Management can be interpreted as a means to reduce liability and reputation damage by reducing expat victimizations. Finally, Remote Management detaches international aid workers from their environment and from beneficiaries. Regardless of these theoretical points of critique, Remote Management will most likely become increasingly popular in the years to come because of continuous technological innovations that reduce adverse components of the strategy.

Chapter 8: Conclusion and discussion

Conclusion

This research aimed to clarify and disentangle the various effects of technological developments on the aid sector's security management strategies and, specifically, Remote Management. The research question, therefore, was formulated as: *How do technological developments affect the security management of aid agencies as well as their views on and their implementations of Remote Management*? To answer this question, this research set out to study 1) aid agency risk perceptions and their relation to security management, 2) the effects of technologies on security management and Remote Management, and 3) the views on and implementations of Remote Management by aid agencies. This research took a 'middle ground' approach, combining both proximate and deep insights on aid agencies' security management. By relating social science theories to empirical findings, this research contributed to the existing literature. Next to the scientific and the grey literature as sources of information, 31 interviews were conducted with security managers and country directors of the ICRC, NGOs and the UN in Afghanistan, Iraq, Somalia, South Sudan and Syria. Skype was used to conduct these interviews. As the main method of data collection, Skype fitted the technology-focused content of the research best.

From risk perceptions to security management

Whereas information tools and undermining technologies pose new risks to aid agencies, the four main categories of risk identified by aid actors are collateral damage, armed groups and terrorism, local politics and crime. In the security management of aid agencies, various technologies have recently been implemented. These technologies include security information-gathering tools (e.g. crowdsourcing via social media) and tracking devices as well as security information-sharing tools (e.g. mapping platforms) and online security trainings. There are also various technologies that improve aid worker security indirectly by reducing their need to be in the field, for instance by using advanced data processing tools (e.g. Artificial Intelligence), satellite assessments, drones, biometric and electronic registration, and online cash transfers. Of course, this reliance on technologies leads to new vulnerabilities against which aid agencies need to protect themselves. Strikingly, virtually all of these technologies improve security via strengthening aid agencies' protection strategies rather than by improving their (preferred) acceptance strategies.

Views on Remote Management

Since conflict areas are becoming increasingly dangerous, Remote Management is more and more likely to be used. Remote Management (here defined as: 'a mode of operation in which international staff, either after relocation, after evacuation or by design, manages a project from a distant location because of high or increasing security risks, while national staff members or local partners implement the project on the ground') may reduce security risks, but it increases other risks to projects (e.g. quality risks). The combination of benefits and challenges of Remote Management has led to ambiguous views of security managers and country directors on the strategy. Some define it as 'another programming modality' with its own limitations and benefits. This view is dominant in areas that are less dangerous, at headquarters and where Remote Management is a relatively new phenomenon. Others, especially in those areas in which Remote Management has been used for decades, mention that it can only be 'a last resort'. They frequently refer to deteriorating program quality and the morally questionable transfer of risks to nationals (although national staff's views are not well-known among managers). The argument of the immorality of a risk transfer can be nuanced by questioning whether risks are actually transferred (or merely change) and whether the change in risk profiles is (necessarily) morally objectionable.

Implementing Remote Management

Irrespective of the doubts and disadvantages, Remote Management is widely used. It is being implemented in all of the conflict settings studied in this research by almost all of the agencies that were interviewed. Next to working through national staff and national partners, various innovative alternatives have been designed and implemented. While the duration of the use of Remote

Management spurs creative approaches (e.g. in Somalia and Afghanistan), the higher risk perceptions (in Syria and Somalia) lead to a more widespread use of Remote Management and the withdrawal of internationals abroad instead of to a safer place in the country. The availability of technologies has reduced the negative ramifications of Remote Management with regard to planning, communication between staff members, the security of national implementers and the ability to monitor. In brief, technologies have made Remote Management much easier and significantly more effective.

Mediating factors

Nature of aid agency

In order to test whether the nature and culture of the aid agency matters for its security management, its use of technologies and its view on and implementation of Remote Management, this research distinguished between three types of aid agencies: the ICRC, NGOs and the UN. The UN consistently perceives risks to be higher and therefore uses more protection and deterrence strategies, whereas the ICRC sees risks generally as less threatening and makes more use of acceptance measures. NGOs report very diverse views. Although a distinction between humanitarian and development NGOs does not provide useful insights, risk perceptions are believed to be higher for Christian NGOs in Islamic countries. In general, all agencies seem to rely mostly on protection measures in the countries of this study, although the ICRC is more likely to also use acceptance measures whereas the UN proves more willing to use deterrence strategies as well.

In general, technologies are not yet used at a very large scale in conflict settings, but they are increasingly often being introduced and developed, even in the most volatile settings. While the ICRC and the UN have conducted some large-scale technological projects, the introduction of relatively basic, security-enhancing technological tools is somewhat lagging behind in comparison with NGOs. Lastly, views on Remote Management are very diverse within the different types of aid agencies, which renders it impossible to draw lines between groups of aid organizations. However, in terms of implementation, the UN is the most conservative agency by almost only using its own staff, while NGOs and the ICRC are more innovative.

Conflict setting

Likewise, different countries with varying conflict settings were identified as possible explanatory factors for the views on security management, technologies and Remote Management. The five conflict settings in this study were Afghanistan, Iraq, Somalia, South Sudan and Syria. Aid agencies in Somalia and Syria tend to view risks as higher and more diverse than elsewhere, which explains the increased use of measures of deterrence and protection (including Remote Management) in these countries. In South Sudan and Iraq, on the other hand, risks are perceived to be relatively low, which leads aid agencies to mostly use acceptance measures, while agencies operating in Afghanistan take a center position.

Aid agencies have been using technologies in all the countries under study, although implementation difficulties (e.g. due to opposition of armed groups and low educational levels) differ somewhat per region, with slightly less use of technologies in Afghanistan and South Sudan. Aid agencies in countries in which Remote Management has a long history (e.g. Somalia and Afghanistan) are more critical of the strategy than agencies in countries in which it has been adopted recently (e.g. South Sudan and Syria). The duration of the use of Remote Management seems to have a positive effect on the development of innovative variants of the strategy (with agencies in Somalia and Afghanistan using the most creative variants). Lastly, it is noteworthy that headquarters' staff is slightly more positive about Remote Management than their field-based colleagues.

The future

Technology

As an essential process of modernization, the rise in the usage of technological tools is unlikely to halt anytime soon. Although technological progress faces downsides (e.g. the use of technologies by threat actors) as well as challenges (e.g. opposition and unfulfilled conditions for implementation), technologies have also outright beneficial effects on aid delivery in conflict settings with regard to efficiency, effectiveness, visualization and democratization. In this line of thought, the integration of various tools in the aid sector's security management is most likely only a prelude to the technologization of the security management of aid agencies in volatile settings.

Remote Management

The fact that Remote Management is used by almost every agency operating in the conflict settings under study is testimony to the influence of technologies on the security (and operational) management of aid agencies. Technologies do not only support protection strategies, but they also enable a broader implementation of the protection strategy by allowing more and more parts of the aid project cycle to be executed remotely and thereby reducing the need for (international) staff to go into the field. Assuming that technological progress will carry on and conflict situations will continue to exist or arise (and there is no reason to doubt any of these two assumptions), Remote Management will be increasingly used and may very well expand to become the primary implementing modality in risky areas.

Theoretical considerations

Social science theories proved to provide useful explanations for the empirical findings of this research. From a Foucauldian point of view, it can be argued that technologies simply enable aid agencies (as the new sovereigns) to wield their biopolitical power over beneficiary populations more easily, while technologies in aid agencies' security management also improve the exercise of disciplinary power over national staff. Taking a Beckian perspectives, the aid sector has become fundamentally risk averse and is ever more preoccupied with minimizing risks in order to guarantee that aid delivery (as a means to protect modernization processes) can continue. Following Beck's predictions, the aid sector will have to update its technologies constantly to enhance the resilience of its technological systems. Interpreting Beck, when aid agencies consider Remote Management, they (will have to) balance the security risks (of field presence) against the quality risks (of field absence).

Next, it can be claimed that Remote Management and technologies politicize aid. In Remote Management, the politicization of aid is symbolized by the shift of decision-making power to Western centers in the global South. In the use of technologies, the Western origins of these tools can be expected to contribute to the image of aid as inherently Western and political. Next, new technologies, due to their military origins, blur the lines between aid and the military and evoke very difficult questions as to the role of aid agencies in conflict settings. Whereas the militarization of aid creates new risks to aid agencies, a resort to deterrence measures may further militarize them and lead to higher risks in turn.

The commercialization of aid is spurred when new technological tools require partnerships between agencies and businesses as well as by the fierce competition among agencies (e.g. over grants). In security management, however, technologies may also lead to better collaboration and reduced competition. Remote Management, as a means to reduce liability and reputation damage, can be seen as a consequence of the commercialization of aid. Also, Remote Management and technologies socially, emotionally and psychologically detach international staff from the field, reducing empathy with and understanding of the security conditions and the beneficiaries' needs. Although some aspects of these theories may overstate the challenges ahead, it is beyond doubt that the aid sector faces some pressing questions in the era of technologization and Remote Management.

Discussion

This research is limited in the sense that it specifically focuses on the relation between technologies, security management and Remote Management. However, the rise of technologies in the aid sector and the progressive use of Remote Management are no stand-alone processes. They change the relations between aid agencies and the outer world (e.g. with beneficiaries, other aid agencies and threat actors) and the relations within the organization (e.g. between international and national staff) as well as the nature of the aid actors and their services. The diverse effects of technologies and Remote Management on agencies' relations with other actors and on the agency itself are worthwhile studying more in-depth.

Since this research is quite explanatory, due to the gap in the literature, it was beyond its scope to study the role of technologies and Remote Management in relation to a social science theory in-depth. Some preliminary observations were made throughout the chapters but these can be elaborated in a future study. For instance, in order to test the Foucauldian assumption that technologies enable aid agencies to better control population, it is worthwhile studying the (change in) interaction between the (international) aid workers and beneficiaries as well as the role of technology in this relation. In addition, a study to test the commonly held belief that the aid sector becomes increasingly more risk averse can be carried out by means of an ethnographic, Beckian study of risks and technologies in aid provision, which would be a refreshing and much needed impetus for the (largely theoretical) debate. Furthermore, practical studies on the roles of technologies and Remote Management could potentially shed interesting lights on the relation between aid and politics, aid and the military, and aid and commercial actors. Whether technologies and Remote Management indeed lead to an expatriate social, psychological and emotional detachment from the field can be tested rather easily through both qualitative and quantitative approaches as well. A research on this detachment and its possible consequences would be highly beneficial to aid agencies since an expatriate detachment from the field would be a well-founded cause for concern regarding the increasing use of Remote Management.

In terms of limitations, the use of technologies in this research (i.e. Skype and e-mail) may have caused some emotional and social distance between the researcher and the interviewees. Nevertheless, frequent e-mail exchange as well as the combination of voice- and audio-transmission led to sufficient trust among interviewees to report sensitive information on the security approaches of their organizations. Also, no discrepancy was experienced in length or quality between Skype-interviews and face-to-face interviews, exemplifying the merits of Skype-interviews and its potential for future studies. This research could have benefitted, however, from Big Data analysis of the 'virtual field' by analyzing online (social media) accounts from security managers and country directors of aid agencies in conflict settings. However, the huge costs of big data software and its relative infancy prevented its use for this research at this stage, but might be an interesting addition to the research in a future research.

Lastly, it is worthwhile mentioning that there is no research as of yet on the implementation process of technologies in aid agencies. It would be very informative to map the proponents and opponents of the technologization of an aid agency. This research could shed some light on (yet unidentified and un(der)exposed) views of aid workers on technologies (and, possibly, on Remote Management). By tracing the decision-making and implementation processes, this research could also provide information on frequently faced hurdles or challenges and thereby help to improve the decision-making on or implementation of future technologically advanced (and remotely managed) projects. In brief, due to the wide gap in the literature on these topics, future researchers have many opportunities. This research offers as a starting point for future research that, although technologies and Remote Management pose some difficult and pressing questions, they will also provide unmatched opportunities in the years ahead and will most likely rise to become ever more important in aid agencies' activities.

Bibliography

Abild, E. (2010). 'Creating Humanitarian Space: A Case Study of Somalia.' *Refugee Survey Quarterly, 29*: 67-102.

Apthorpe, R. (2011). 'Coda: With Alice in Aidland: a seriously satirical Allegory'. In: Mosse, D. (ed.) *Adventures in Aidland: The Anthropology of Professionals in International Development* [199-220]. New York: Berghahn books.

Armstrong, J. (2013). *The Future of Humanitarian Security in Fragile Contexts*. European Interagency Security Forum (EISF).

Babbie, E. (2010). *The Practice of Social Research*. Belmont: Wadsworth.

Barakat, S. and Ellis, S. (1996). Researching under fire: Issues for consideration when collecting data and information in war circumstances, with specific reference to relief and reconstruction projects. *Disasters, 20:* 149-156.

Beck, U. (1992). *Risk Society: Towards a New Modernity.* London: Sage Publications.

Beck, U. (2006). 'Living in the world risk society.' *Economy and Society, 35*: 329-345.

Belliveau, J. (2013). ''Remote management' in Somalia.' *Humanitarian Exchange Magazine, 56*: 25-27.

Bollettino, V. and Bruderlein, C. (2008). 'Training humanitarian professionals at a distance: testing the feasibility of distance learning with humanitarian professionals.' *Distance Education, 29*: 269-287.

Borland, K. (1991). “That’s not what I said”: interpretative conflict in oral narrative research. In: Gluck and Patai (Eds.) *Women’s words: the feminist practice of oral history*. Routledge: 63-75.

Brabant, K. van (2012). *Incident Statistics in Aid Worker Safety and Security Management: Using and Producing Them*. EISF: European Interagency Security From.

Byrne, R. (2014). 'Trends in Intelligence Gathering by Governments.' *European Interagency Security Forum*: 12-16.

Candy, P. (2014). *Humanitarians under attack: Delivering Aid in Insecure Settings.* ATHA podcast: 20-11-14.

Canter, D.V. and Sarangi, S. (2009) 'The rhetorical foundation of militant jihad.' In: Canter, D.V. (ed.) *Faces of Terrorism: Multidisciplinary Perspectives* [35-61]. Chihester: Wiley-Blackwell.

Carle, A. and Chkam, H. (2006). *Humanitarian action in the new security environment: policy and operational implications in Iraq*. London: HPG background paper.

Cater, J. (2011). 'Skype: A cost effective method for qualitative research.' *Rehabilitation Counselors & Educators Journal, 4*: 3.

Collinson, S. and Duffield, M. (2013). *Paradoxes of presence: Risk management and aid culture in challenging environments*. London: Humanitarian Policy Group.

Costa, D. (2012). *Working in Challenging Environments: Risk Management and Aid Culture in South Sudan: Field report South Sudan*. Humanitarian Policy Group (ODI) and University of Bristol research project.

Creswell, J.H. (2003). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Thousand Oaks: Sage Publications Inc.

Dandoy, A. and Pérouse de Montclos, M.-A. (2013). 'Humanitarian workers in peril? Deconstructing the myth of the new and growing threat to humanitarian workers.' *Global Crime, 4*: 341-358.

Deakin, H. and Wakefield, K. (2013). 'Skype interviewing: reflections of two PhD researchers.' *Qualitative Research, 14*; 603-616.

DFID (2015). *Cross Cutting Evaluation of DFID's Approach to Remote Management in Somalia and North-East Kenya. Evaluation report*. Integrity Research and Consultancy and Axiom Monitoring and Evaluation.

Digital Humanitarian Network (2015). *Purpose.* Retrieved from: http://digitalhumanitarians.com/about (20-05-15).

Donini, A. and Minear, L. (2006). *Humanitarian Agenda 2015: Principles, Power, and Perceptions*. Medford: Feinstein International Center.

Donini, A. and Maxwell, D. (2013). 'From Face-to-Face to Face-to-Screen: Implications of Remote Management for the Effectiveness and Accountability of Humanitarian Action in Insecure Environments'. *International Review of the Red Cross, 95*: 384-413.

Duffield, M. (1997). 'NGO relief in war zones: Towards an analysis of the new aid paradigm.' *Third World Quarterly, 18*: 527-542.

Duffield, M. (2012). 'Challenging Environments: Danger, resilience and the Aid Industry'. *Security Dialogue, 43*: 475-492.

ECHO (2013). *Instruction note for ECHO staff on Remote Management*. Brussels: Directorate-General Humanitarian Aid and Civil Protection.

Egeland, J., Harmer, A. and Stoddard, A. (2011). *To Stay and Deliver. Good practice for Humanitarians in complex security environments.* OCHA: Policy and Studies Series.

EISF (2010). *The Information Management Challenge: A Briefing on Information Security for Humanitarian Non-Governmental Organisations in the Field*. European Interagency Security Forum.

EISF (2012). *Security Management and Capacity Development: International agencies working with local partners.* European Interagency Security Form (EISF).

EISF (2014). *Communications Technology and Humanitarian Delivery: Challenges and Opportunities for Security Risk Management*. European Interagency Security Forum (EISF).

Fast, L.A. (2010). 'Mind the gap: Documenting and explaining violence against aid workers.' *European Journal of International Relations, 16*: 365-389.

FSAC (2013). *Beneficiary feedback and complaint mechanism*. Food Security and Agriculture Cluster, Afghanistan.

Foucault, M. (2003). *Society Must Be Defended. Lectures at the Collège de France, 1975-1976*. New York: Picador.

Foucault, M. (2015). '*Le discours ne doit pas être pris comme...'*. Retrieved from: http://1libertaire.free.fr/MFoucault441.html (24-06-15).

Fujii, L. A. (2009). 'Interpreting truth and lies in stories of conflict and violence.' In: Chandra Lekha Sriram, John C. King, Julie A. Mertus, Olga Martin-Ortega and Johanna Herman (Eds.) *Surviving Field Research: working in violent and difficult situations* [147-162]. New York: Routledge.

Gilman, D. (2014). 'Cyber-Warfare and Humanitarian Space'. *European Interagency Security Forum*: 8-11.

Graham, S. (2011). *Cities Under Siege: The New Military Urbanism.* London: Verso.

Guba, E.G. and Lincoln, Y.S. (1994). 'Competing paradigms in qualitative research.' In: N.K. Denzin and Y.S. Lincoln (Eds.) *Handbook of qualitative research* [105-117]. Thousand Oaks: Sage.

Gundel, J. (2006). *Humanitarian action in the new security environment: policy and operational implications in Somalia and Somaliland*. Humanitarian Policy Group: HPG Background Paper.

Gupta, A., Lamba, H., Kumaraguru, P. and A. Joshi (2013). 'Faking sandy: characterizing and identifying fake images on Twitter during hurricane sandy.' In: *Proceedings World Wide Web, 2013*: 729–736.

Hansen, G. (2008). 'Series of Briefing Papers on NGOs' and others' humanitarian operational modalities in Iraq.' *NGO Coordination Committee in Iraq.*

Harmer, A., Stoddard, A. and Toth, K. (2013). *Aid Worker Security Report. The New Normal: Coping with the kidnapping threat.* Humanitarian Outcomes.

Hilhorst, D. and Jansen, B. (2005). *Fieldwork in Hazardous Areas*. Wageningen: Wageningen University.

Hilhorst D. and Jansen, B. (2010). 'Humanitarian space as arena: a perspective on the everyday politics of aid.' *Development and Change, 41*: 1117–1139.

Howe, K., Stites, E. and Chudacoff, D. (2015). *Breaking the Hourglass: Partnerships in Remote Management Settings - The Cases of Syria and Iraqi Kurdistan*. Somerville: Feinstein International Center.

HPN (2010). *Operational security management in violent environments. Good Practice Review: Number 8.* London: Humanitarian Practice Network.

Humanitarian OpenStreetMap Team (2015). *About*. Retrieved from: http://hotosm.org/about (08-05-15).

Humanitarian Outcomes (2015). *Aid Worker Security Database*. Retrieved from: https://aidworkersecurity.org/incidents (01-05-15).

ICRC (2015). *Mandate and Mission.* Retrieved from: https://www.icrc.org/en/mandate-and-mission (04-03-15).

IFRC (2013). *World Disasters Report 2013: Focus on technology and the future of humanitarian action*. Geneva: IFRC.

Janghorban, R., Roudsari, R.L. and Taghipour, A. (2014). 'Skype interviewing: The new generation of online synchronous interview in qualitative research.' *International Journal of Qualitative Studies on Health and Well-Being, 9.*

Kaiser, J. and Fielding, R. (2014). 'A Principled Approach to Data Management.' *European Interagency Security Forum*: 37-41.

Kant, I. (2004). *Critique of Practical Reason.* Mineola: Dover Publications Inc.

Karlsrud, J. and Rosén, F. (2013). 'In the Eye of the Beholder? The UN and the Use of Drones to Protect Civilians.' *Stability: International Journal of Security & Development, 27*: 1-10.

Katz, R. (2014). *Follow ISIS on Twitter: A Special Report on the Use of Social Media by Jihadists.* Retrieved from: http://news.siteintelgroup.com/blog/index.php/entry/192-follow-isis-on-twitter-a-special-report-on-the-use-of-social-media-by-jihadists (01-05-15).

Mayo, A. (2014). 'SMS Technology and Bulk SMS Delivery Systems.' *European Interagency Security Forum*: 46-50.

Meier, P. (2011). 'New information technologies and their impact on the humanitarian sector.' *International Review of the Red Cross, 93*: 1239-1263.

Meier, P. (2015a). *Digital Humanitarians: How Big Data Is Changing the Face of Humanitarian Response*. Boca Raton: CRC Press.

Meier, P. (2015b). *Humanitarian UAV Missions in Nepal: Early Observations*. Retrieved from: http://irevolution.net/2015/05/03/humanitarian-uav-missions-nepal/ (20-05-15).

Metcalfe, V., Martin, E. and Pantuliano, S. (2011). *Risk in humanitarian action: towards a common approach*? London: HPG Commissioned Paper.

Minei, E. and Matusitz, J. (2012). 'Cyberspace as a new arena for terroristic propaganda: an updated examination', *Poiesis Prax, 9*: 163-176.

Montclos, M.A.P. (2014). 'The (de)Militarization of Humanitarian Aid: A Historical Perspective.' *Humanities, 3*: 232-243.

Musila, G.M. (2013). 'Early Warning and the Role of New Technologies in Kenya.' In: Mancini, F. (ed.) *New Technology and the Prevention of Violence and Conflict* [42-55]. New York: International Peace Institute.

Norman, B. (2012). *Monitoring and accountability practices for remotely managed projects implemented in volatile operating environments*. Tearfund.

NSP (2015). *NSP Services at a glance*. Retrieved from: http://www.nspsomalia.org/joomla/index.php/about-nsp/nsp-services-at-a-glance (05-03-15).

Palacios, G. de, and (2014). 'Applicability of Open Source Systems (Ushahidi) for Security Management, Incident and Crisis Mapping.' *European Interagency Security Forum*: 51-55.

Pérouse de Montclos, M.-A. (2014). 'The (de)Militarization of Humanitarian Aid: A Historical Perspective.' *Humanities, 3*: 232-243.

Persaud, C. (2014). *NGO Safety and Security Training Project*. EISF and Interaction.

Porter, B. and Emmens, B. (2009). *Approaches to Staff Care in International NGOs*. People in Aid and Interhealth.

Powell, C. (2001). *Remarks to the National Foreign Policy Conference for Leaders of Nongovernmental Organizations*. Retrieved from: http://avalon.law.yale.edu/sept11/powell_brief31.asp (03-06-15).

Rachels, J. and Rachels, S. (2009). *The Elements of Moral Philosophy.* New York: McGraw-Hill Education.

Rothstein, H.R. and Hopewell, S. (2009). 'Grey Literature'. In Cooper, H., Hedges, L.V. and Valentine, J.C. (eds.) *The Handbook of Research Synthesis and Meta-Analysis. Second Edition* [103-128]. New York: Russell Sage Foundation.

Sambuli, N. and Awori, K. (2014). 'Monitoring Online Dangerous Speech in Kenya: Insights from the Umati Project.' *European Interagency Security Forum*: 27-31.

Sandvik, K.B. and Lohne, K. (2014). 'The Rise of the Humanitarian Drone: Giving Content to an Emerging Concept.' *Millennium - Journal of International Studies*: 1-20.

Security Management Initiative (2009). *Cyber Security for International Aid Agencies: A Primer*. SMI Professional Development Brief 3.

Sheik, M., Gutierrez, M.I., Bolton, P., Spiegel, P., Thieren, M. and Burnham, G. (2000). 'Deaths among humanitarian workers.' *BMJ, 321*: 166-168.

Somalia NGO Consortium (2009). *Remote Programming Modalities in Somalia.* Discussion paper.

Souness, C. (2011). *Beneficiary Accountability in Remote Managed Locations: An assessment of Tearfund's monitoring & accountability practices*. Tearfund Afghanistan.

Steets, J., Reichhold, U. and Sagmeister, E. (2012). *Evaluation and review of humanitarian access strategies in DG ECHO funded interventions*. Global Public Policy Institute: ECHO report.

Stoddard, A. (2003a). 'Humanitarian NGOs: challenges and trends.' In: Macrae, J. and Harmer, A. (Eds.) *Humanitarian action and the 'global war on terror': a review of trends and issues*. London: Humanitarian Policy Group.

Stoddard, A. (2003b). 'With us or against us? NGO neutrality on the line.' *Humanitarian Exchange Magazine, 25*: 5-7.

Stoddard, A. and Harmer, A. (2010). *Supporting Security for Humanitarian Action. A review of critical issues for the humanitarian community*. Humanitarian Outcomes.

Stoddard, A., Harmer, A. and DiDomenico, V. (2009). *Providing aid in insecure environments: 2009 update: Trends in violence against aid workers and the operational response*. London: HPG Policy Brief 34.

Stoddard, A., Harmer, A. and Haver, K. (2006). *Providing aid in insecure environments: trends in policy and operations*. London: HPG report 23.

Stoddard, A. Harmer, A. and Renouf, J.S. (2010). *Once Removed: Lessons and challenges in remote management of humanitarian operations for insecure areas*. Humanitarian Outcomes.

Stoddard, A., Harmer, A. and Ryou, K. (2014). *Unsafe Passage: Road attacks and their impact on humanitarian operations*. Humanitarian Outcomes.

Tafere, M., Katkiwirize, S., Kamau, E.N. and Nsabimana, J. (2014). 'Mobile Money Systems for Humanitarian Delivery.' *European Interagency Security Forum*: 42-44.

Thomas, W.I. (1928). *The Child in America.* New York: Alfred A. Knopf.

UN (2008). *Wireless Technology for Social Change: Trends in Mobile Use by NGOs*. Washington DC: United Nations Foundation.

UNHCR (2003). *Iris testing of returning Afghans passes 200,000 mark*. Retrieved from: http://www.unhcr.org/3f86b4784.html (20-05-15).

UNHCR (2012a). *Modern technology helps meet the needs of refugees in South Sudan*. Retrieved from: http://www.unhcr.org/50dc5a309.html (20-05-15).

UNHCR (2012b). *UNHCR distributes biometric ID cards to refugees in Senegal*. Retrieved from: http://www.unhcr.org/508536389.html (21-05-15).

UNOCHA (2013). *Humanitarianism in the Network Age*. New York: United Nations.

UNOCHA (2015). *Information Management.* Retrieved from: http://www.unocha.org/what-we-do/information-management/overview (29-04-15).

UNOSAT (2011). *UNOSAT Brief. Satellite Applications for Human Security*. Retrieved from: http://www.unitar.org/featured/unosat-brief-2011-focuses-satellite-applications-human-security (20-05-15).

Windt, P. van der, and Humphreys, M. (2015). 'Crowdseeding Conflict Data'. *Journal of Conflict Resolution* [Forthcoming].

Žižek, S. (2009). *First as Tragedy, Then as Farce*. Retrieved from: https://www.thersa.org/discover/videos/event-videos/2009/11/first-as-tragedy-then-as-farce/ (04-06-15).

Annex I: List of interviews

#	Title	Country	Agency	Name	Communication
1	Anonymous	Afghanistan	-	-	Face-to-face
2	Anonymous	Afghanistan	-	-	Skype
3	Anonymous	Iraq/Syria	-	-	Skype
4	Anonymous	Somalia	-	-	Skype
5	Anonymous	South Sudan	-	-	Skype
6	Senior official	Somalia	ICRC	-	Skype
7	Senior official	Syria	ICRC	-	Skype
8	Senior official	Iraq	ICRC	-	Skype
9	Senior official	International	UN	-	Face-to-face
10	Senior official	Somalia	UN	-	Skype
11	Security Focal Point	International	UNDPA	-	Face-to-face
12	Security Focal Point	International	UNDP	Vandamme	Face-to-face
13	Senior Field Security Advisor	Somalia	UNDP	-	Skype
14	Country Director	Somalia	INGO	-	Skype
15	Country Director	Somalia	INGO	-	Skype
16	Country Director	Iraq	INGO	-	Skype
17	Country coordinator	Somalia	INGO	-	Skype
18	Country Director	Somalia	Medair	-	Skype
19	Senior Country Security Advisor	South Sudan	INGO	-	Skype
20	Security Focal Point	Somalia	INGO	-	Skype
21	Security Focal Point	South Sudan	NGO Forum	Lidstone	Skype
22	Field Security Officer	Syria	World Vision	-	Skype
23	Security Advisor	Somalia	World Vision	Domrachev	Skype
24	Safety and Security Manager	Iraq	Save the Children	Lancaster	Skype
25	Security Advisor	Afghanistan	NRC	-	Skype
26	Security Manager	International	RedR	-	Skype

27	Global Security Focal Point	International	ICCO	Pijpker	Skype
28	Senior Advisor Security and Risk Management	Somalia	GIZ	Schwarz	Skype
29	Technical and Innovation Officer	International	Medair	-	Skype
30	CEO	International	Centre for Safety and Development	Brons	Face-to-face
31	Risk Management Consultant	Somalia	Independent	-	Skype

Annex II: Interview guide

Obviously, interview questions were adapted to the interviewees background, role and operating environment. For instance, while security managers were better positioned to share their views on the risks in their environment, the resilience of the aid agency and Remote Management as a strategy, country directors were better able to provide insights on the aid agency's view on technologies and the implementation of remotely managed projects. Moreover, experts are usually specialized in a very specific field on which the questions as a consequence need to focus, while heads of the security forums can share insights on their member's security policies from a more neutral perspective than their members themselves. The following main topics were identified as leading issues in the interviews:

1. Aid actor and self-image
    - What are your responsibilities?
    - Which projects does your organization run?
    - What is your mandate?
    - How does your organization differ from others?

2. Risk perception
    - Which threats do your staff face?
    - Who poses these threats?
    - In your view, why do they threaten you?
    - Which staff is at risk?

3. Resilience and security strategies
    - How do you improve the security of your staff?
    - Which acceptance measures do you use?
    - Which protection measures do you use?
    - Which deterrence measures do you use?

4. Technology
    - How do you gather security information?
    - How do you communicate with field staff?
    - How does your work differ from five, ten years ago?
    - In what ways do you use new technologies?
    - How do you plan on using new technologies in the future?

5. View on Remote Management
    - How often do you evacuate internationals/relocatables?
    - How would you define Remote Management?
    - What is your view on Remote Management?
    - In how many projects are you working through local partners or local NGOs?
    - According to you, under what conditions is Remote Management appropriate?

6. Implementation of Remote Management
    - Which factors determine the success of a remotely managed project?
    - What are the main challenges in remotely managed projects?
    - Which technologies do you use in remotely managed projects?
    - How do you monitor and evaluate remotely managed projects?
    - What are you responsibilities in terms of the security of the implementers?
    - How do you think local staff looks at remotely managed projects?

Annex III: Coding system