Kalkman *Journal of International Humanitarian Action* (2018) 3:1
DOI 10.1186/s41018-018-0029-4

Journal of International Humanitarian Action

RESEARCH ARTICLE Open Access

Practices and consequences of using humanitarian technologies in volatile aid settings

Jori Pascal Kalkman[1,2,3]

Abstract

This article presents the results of an exploratory study into aid agencies' use of technologies for security purposes. Since there appears to be a consensus in the aid sector that areas of operations are increasingly dangerous, aid agencies are upgrading their security strategies by adopting technological innovations. I conducted Skype interviews with security managers and country directors responsible for operations in dangerous countries. These interviews show that humanitarian technologies are more and more used in volatile countries for security reasons. In this light, I empirically assess the critique of some academics (1) that risks are not mitigated but transferred to more vulnerable actors, (2) that technology is not a neutral fix but has local political repercussions, and (3) that international and national aid workers grow increasingly distant from their local counterparts and the people they aim to help. This article contributes to the literature by critically re-evaluating and nuancing these critiques.

Keywords: Humanitarian technologies, Remote management, Security management, Aid sector, Risk, Local politics, Distancing

Introduction

The areas in which aid workers are operating can be extremely volatile and appear to be much more dangerous than a few decades ago. Sheik et al. (2000), for instance, studied aid worker deaths in the period from 1985 to 1998 and report fewer than 40 casualties per year (except for 1993 and 1994). The latest Aid Worker Security Report, however, demonstrates that in the last 10 years, the number of intentional aid worker deaths never dropped below 70. In 2016 alone, 288 aid workers were victimized in 158 attacks (Stoddard et al. 2017:2). Although the relative numbers may look different (as the total number of aid workers is likely to have increased as well), there is general consensus that "humanitarian contexts have become increasingly dangerous for humanitarian agencies" (Cunningham 2017:1).

The reasons for such violence may be various. They can root in the jihadist battle against the West in general, including international non-governmental organizations (NGOs) and the United Nations (UN) (see Canter and Sarangi 2009), which accounts for attacks on aid workers by the Islamic State of Iraq and the Levant (ISIL) and the Taliban. Others state that attacks against aid agencies are a result of the blurring of lines between Western security (or political) interests and humanitarian or development aid, leaving aid workers more vulnerable to attacks by those opposing these Western interests (Collinson and Duffield 2013; Duffield 2010; Egeland et al. 2011). Former Secretary of State Colin Powell's (2001) depiction of NGOs as "a force multiplier for us, such an important part of our combat team" is seen as indicative of this trend, just like the attacks on the UN and the International Committee of the Red Cross (ICRC) in the wake of the 2003 Iraq invasion. Lastly, a considerable number of attacks are also economically motivated or have local political reasons and can therefore be attributed to "criminals," dissatisfied opposition, or ethnic groups (Abild 2010; Gundel 2006).

Correspondence: j.p.kalkman@vu.nl
[1]Department of Organization Sciences, VU University, De Boelelaan 1105, 1081HV Amsterdam, The Netherlands
[2]Department of Management, Organisation and Defence Economics, Netherlands Defence Academy, De la Reyweg 120, 4818BB Breda, The Netherlands
Full list of author information is available at the end of the article

In response to these threats, aid agencies have three basic strategies which are often used in coalescence to enhance their overall security. This "security triangle" includes acceptance, protection, and deterrence (HPN 2010). Ideally, aid agencies rely primarily on acceptance strategies (HPN 2010:56). This security strategy aims to reduce the threats against an agency by building support for its projects and programs among the community in which the organization is working (Cunningham 2017). Protection, in line with the conventional interpretation of the word, refers to strategies that reduce the vulnerability of the organization: it can include using bunkers and armed vehicles or removing logos and going undercover (HPN 2010). The final security strategy, and usually a last resort option, is deterrence, in which an organization takes measures to deter threats, usually taking the form of armed guards or the threat of withdrawal (ibid.). Even though acceptance is the preferred strategy (Fast et al. 2013), aid agencies in some settings are believed to increasingly rely on protection and deterrence measures instead (Schneiker 2013).

Technologies could contribute to all these strategies and help aid agencies to keep their staff safe from external threats. But what does "technology" mean in this context? Humanitarian technology refers to technologies developed and adopted in the humanitarian sector in the past decades. It includes both basic and complex technologies, thus varying from mobile phones, online cash transfers, and social media to biometrics identification, geospatial mapping, drones, and big data (Sandvik et al. 2014; Sandvik and Lohne 2014; Duffield 2013; Karlsrud and Rosén 2013). Some humanitarian technologies can also specifically be used for security purposes, for instance to collect or relay security information. Examples include incident mapping, serious gaming for security training purposes, and sending security updates as text messages (Mayo 2016; De Palacios 2016; Gonsalves 2016).

Combining these humanitarian technologies with the security triangle of acceptance, protection, and deterrence, organizations can broadcast and promote their programs and projects online via various fora to expand people's understanding of their activities and build goodwill. Aid agencies can also employ basic communication technologies to crowdsource security information from the field to enhance their overview of volatile areas and to protect staff by pulling them back when a situation deteriorates (see Van der Windt and Humphreys 2016). Deterrence, additionally, can be modernized by the online communication of threats of withdrawal if aid workers are threatened or hurt.

The significant contributions that technological progress can make to humanitarian action in general are widely acknowledged. Publications on good practices of technology use abound. Exemplary, the International Federation of the Red Cross published its 2013 World Disaster Report with the telling subtitle "Focus on technology and the future of humanitarian action". In fact, there are numerous publications that share aid agencies' success stories and lessons learned with regard to the use of humanitarian technologies (e.g., UNOCHA 2013; Vazquez Llorente and Wall 2016; Meier 2011). In this paper, I am specifically interested in studying the interface between security management and technological progress. Even though both the importance of aid agency security management (HPN 2010; Egeland et al. 2011; Collinson and Duffield 2013) and the relevance of technological progress in the aid sector (e.g., IFRC 2013; UNOCHA 2013) are studied on their own, security management and technological progress are only infrequently studied in junction.

When humanitarian technology in aid agency security management is studied, either one of two strands of research can be recognized. Firstly, there are very practical studies which share (usually in a few pages) an aid agency's experiences with using a certain humanitarian technology for security purposes and what lessons others can learn from it (Vazquez Llorente and Wall 2016). The second strand of research is academic and provides fundamental explanations of aid agencies' security situations and security management in dangerous areas. In particular, researchers focus on aid agencies' tendency to physically and psychologically withdraw from the field, which they perceive as increasingly dangerous, and their subsequent resort to humanitarian technologies to keep control over operations (e.g., Andersson and Weigand 2015; Duffield 2012, 2013, 2016). While the former strand displays little reference to academic work or theoretical explanations, the latter strand explains fundamental processes with limited reference to empirical data. This is also referred to as an "epistemic gap" between the practical experiences and the fundamental explanations (see Fast 2010). I will therefore study how aid agencies use humanitarian technologies in response to rising risk perceptions as well as the implications of this trend to validate and refine existing fundamental explanations in an attempt to bridge this gap. In this way, I intend to contribute to the "critical scholarly engagement with the humanitarian turn to technology" (Sandvik et al. 2014:222).

Theory

Technological appropriation by humanitarian agencies is not uncontested. On the basis of the critical literature, three prominent fundamental critiques can be distilled. These are summarized here, after which propositions are derived which will be tested on the basis of empirical data. Firstly, the reliance on technologies is believed to be part of aid agencies' increasing risk aversion

(Collinson and Duffield 2013; Duffield 2010), even though technologies do not fundamentally reduce risks. Instead, as Ulrich Beck (1992:19) claims, technological developments are the main cause of risks in modern society. He shows that every new innovation brings its own new risks that have to be resolved subsequently to maintain the system's resilience. Since actors in modern society rely on scientific and rational approaches to prevent and reduce risks as much as possible, Beck (2006:332) concludes that any actor in our society is "increasingly occupied with debating, preventing and managing risks that it itself has produced."

This preoccupation of humanitarian agencies led Collinson and Duffield (2013) to argue that agencies appear more worried about security risks to themselves than about the risks that their beneficiaries are facing. By extension, since large aid agencies are able to use humanitarian technologies for hardening them as a target, other humanitarians and local populations come to be relatively more at risk (Simpson 2015). In this regard, Beck (1992) claims that there is a correlation between poverty and risk, with marginalized actors facing higher risks and being more likely to be hit. From this perspective, the technology-facilitated international and national staff removal from the field has been criticized by scholars for resulting in a risk transfer to local staff members (see Collinson and Duffield 2013; Sandvik 2016). Thus, the first two propositions are:

Proposition 1a: The use of humanitarian technologies in security management does not reduce risks.

Proposition 1b: The implementation of humanitarian technologies in security management shifts risks to more vulnerable actors.

This conclusion feeds into a second critique on humanitarian technology use as a response to security risks. Technological innovations should not be viewed as apolitical or neutral solutions to complex humanitarian problems. The introduction of certain technological solutions to security problems may well rely on oversimplifications of humanitarian challenges, thereby ignoring the complex environments in which humanitarians operate (see Abdelnour and Saeed 2014). Beyond practical questions as the legal and operational consequences of using humanitarian technologies (Meier 2011; Qadir et al. 2016), there are more fundamental problems with viewing a technological solution as the application of a neutral "fix" for a variety of problems (Jacobsen 2015).

In fact, technologies will considerably influence the local, political relations and thereby restructure or transform the (social) field of operations itself. The "humanitarian space" as an area in which humanitarian organizations can safely provide their non-political goods and services is a fiction (Hilhorst and Jansen 2010; Abild 2010). Any humanitarian action will have its repercussions on the local distribution of resources and local power relations. Even though agencies may aim to be neutral, impartial, and independent, they cannot avoid operating in a "humanitarian arena" in which actors based on their views and interests aim to influence the effects of the agencies' operations (Hilhorst and Jansen 2010). Thus, technology "will not save humanitarians from dangerous politics, or from politics in general" (Sandvik et al. 2014:228). Instead, "humanitarian uses of new technology can add to (rather than reduce) the ways in which humanitarian practices are linked to contextual political dynamics" (Jacobsen 2015:2). Thus, the next proposition is:

Proposition 2: Humanitarian technology is not a neutral fix for security problems but has political ramifications.

Understanding local politics is complicated when one is removed from the field, which brings us to the final fundamental critique on the increasing humanitarian reliance on technologies. Donini and Maxwell (2013:385) state that "[t]here also seems to be a correlation between the increase in remote management and the development and generalised availability of a number of distance technologies." Various scholars and professionals have come up with different definitions of Remote Management (see Carle and Chkam 2006; Donini and Maxwell 2013; Egeland et al. 2011; Sandvik 2016; Steets et al. 2012; Stoddard et al. 2010). Combining their insights, I define Remote Management as a mode of operation in which (inter)national staff, either after relocation, after evacuation, or by design, manages a project from a distant location because of high or increasing security risks, while local staff members or local partners implement the project on the ground. This programming modality is not necessarily technology-based itself as it has been used for decades in low-technology countries (Stoddard et al. 2010). Nevertheless, humanitarian technologies reduce the challenges and make it an easier way of operating (see Sandvik et al. 2014, 2016).

Duffield (2012) sees Remote Management as a paradoxical trend of risk-averse Western interventionists who both increase their presence in dangerous areas and at the same time withdraw themselves into remote, safe spaces. Overcoming reduced field interaction and understanding, humanitarian technologies are adopted (see Andersson and Weigand 2015). However, this "cyber-humanitarianism" is believed to only enable a virtual presence and facilitate an epistemological and existential distancing (Duffield 2013, 2016). This may over time result in a loss of relations, knowledge, credibility, and

legitimacy (Sandvik 2016:26). Thus, creating proximity through technology is not unsurprisingly labelled as an illusion (Andersson and Weigand 2015). The increased distance between staff members as well as between bunkerized staff and communities is not only epistemological and existential but also social and emotional. In fact, the traditional humanitarian reliance on empathy and humanity risks to be sacrificed through the absence of face-to-face interaction and due to the digitalization of proximity (Donini and Maxwell 2013). Exemplary, Sandvik (2017:8) quotes one NGO as saying, "If you skip the proximity and empathy with victims of disasters, humanitarianism loses its sense." Thus, our final two propositions are:

Proposition 3a: Remote Management, as a security strategy, fosters the introduction of humanitarian technologies.

Proposition 3b: Humanitarian technologies distance international and national aid workers from the field.

In short, these fundamental critiques on using humanitarian technology for security purposes claim that technologies do not necessarily reduce risks as they create new ones and shift risks to marginalized actors, that technologies are no neutral fixes but will considerably bear on local political relations, and that technology, spurred by Remote Management modalities, facilitates epistemological, existential, and social removal from the field, thereby distancing humanitarians from the communities they are helping. After briefly reflecting on the data collection and analysis, I will discuss how aid agencies use humanitarian technologies in unsafe countries by empirically re-evaluating these theory-based propositions. Then, I reflect on the deeper consequences of my findings by discussing the contribution to existing theories. A concluding paragraph summarizes the findings and sketches the implications.

Data

The data for this research was collected by means of 31 semi-structured, in-depth interviews. By asking open-ended questions, the respondents were enabled to elaborate on how they viewed their own role and identity, what risks they perceived in their operational environment, why their organization used certain technologies for their security management, what they considered to be the main benefits and challenges of using these technologies, and how they viewed and used Remote Management (see Appendix 1 for a general interview guideline). In follow-up questions, respondents were invited to reflect on the deeper consequences of employing these upgraded security strategies (e.g., relation to the field, the future of humanitarian action).

I selected respondents from different types of aid agencies (i.e., ICRC, UN, NGOs) to ensure a representation of general trends within the aid sector. The majority of interviewees were tasked with security management tasks: most were the primary responsible persons for the security management of their organization in a country of operations while a few were general security managers of their organizations and working in headquarters. Apart from security managers, I also interviewed several country directors in case they were also responsible for the security of their staff in the country (since not every organization had a separate security manager in every country).

All respondents were working in or on their agencies' operations in one of the following five countries: Afghanistan, Iraq, Somalia, South Sudan, and Syria. The main reason for choosing these five countries as contexts is that they consistently rank among the most dangerous countries.[1] These countries host a mix of different threats varying from global jihadist groups (e.g., ISIL in Iraq and Syria) to criminality (e.g., Somali pirates) and from a civil war (e.g., South Sudan) to an internationalized war (e.g., Iraq) (see also Stoddard et al. 2017). In the volatile countries of this study, security managers and country directors used various innovations. They identified a range of technologies that were instrumental to keeping activities running without continued physical field presence of expatriate or senior national staff. At the same time, Remote Management was used in all these countries as a (or even the main) programming modality.

Almost all interviews were conducted via Skype for two reasons. A practical reason was that studying aid agency security management in dangerous countries comes with serious logistical complications. Many of the locations from which respondents were working were very difficult or time-consuming to reach (see Cater 2011; Deakin and Wakefield 2014). This might also have distracted security managers or country directors from their core responsibilities and thereby conflicted with the "do-no-harm principle" of doing research in conflict settings. A second, more fundamental reason, for using Skype is that, content-wise, using Skype matches the research perfectly (see Janghorban et al. 2014). In a research on the use of technologies, using a technology is a logical choice. In fact, much of the ordinary work-related communication of these professionals is by means of Skype, so using this means of communication was a way to join their "virtual field."

Except for one interview, all interviews were recorded. Subsequently, the interviews were transcribed and completed with notes of other non-verbal communication. Non-verbal communication, also called meta-data, refers to information derived from the interview other than

what respondents said (Fuji 2009). Although Skype may complicate the retrieval of body language or facial expressions as additional information (due to bad connectivity), silences and refusals to answer questions were insightful in this study.

The combination of transcripts and non-discursive information made over 250 pages of data. This data was uploaded and analyzed by means of qualitative data analysis software (Atlas.ti). The analysis started with the identification of themes based on the propositions (i.e., humanitarian technology in relation to risk reduction, risk shifting, local politics, Remote Management, and distancing). I sought for respondents' associations with these themes and for patterns of relations between these concepts (Miles et al. 2013). This approach helped me to clarify the links between perceived threats, technology use, risks, local politics, and Remote Management and improved my understanding of the implications of security management decisions (e.g., going remote) as experienced by security managers and country directors. The process was iterative, and coding was refined over time to become more specific and precise.

To ensure data quality (Miles et al. 2013), interview findings were compared to the data and findings in reports and guidelines by humanitarian agencies, think tanks, and donors. Next to this triangulation, I dived into deviant cases (e.g., little technology use in remotely managed operations in Somalia) to better understand the variation. Lastly, all respondents have been invited to reflect on their contributions to the analysis, which some of them used to nuance or refine my conclusions. This analysis process enabled a clear and comprehensive overview of aid agencies' uses of technologies in their security management and facilitated a thorough analysis of the fundamental effects.

Findings

In this first section of the findings, I identify and describe briefly which humanitarian technologies aid agencies use for security reasons and how they use these tools in the areas in which they operate. I believe this provides a relevant basis and contextualization for the empirical assessment of the propositions in the next section. Broadly speaking, humanitarian technologies have been adopted for security purposes in two ways: they have been integrated in aid agencies' security management as security tools and they have enabled staff removal from the field (i.e., a protection strategy).

Humanitarian technologies used for aid agency security management can be grouped into two main categories. Firstly, information technologies are employed for collecting security information. One possibility for this is to provide all staff with mobile phones and smart phones to keep them up to date about security developments from the field. Another option is crowdsourcing in which public information is used for building situation awareness of the security conditions. In this case, agencies rely on local information by tracing local media or following what inhabitants share on social media. On a basic level, one security manager, for instance, mentioned that he followed the battle for Kirkuk live on Twitter. Specific security information can also be collected through tracking devices. Given that many security incidents happen on the road, aid agencies track their vehicles when staff are going into the field, so that travelling staff can be geolocated at any moment. Apart from information-gathering, technological progress is employed for sharing security information to people in the field. Prominently, online platforms can be used in which security managers can enter security incidents which can be subsequently checked by other users. Security managers also mention the use of Skype, smart phone apps, and SMS text messages to disseminate security information. A more enduring and comprehensive way of sharing security-relevant information to people working in the dangerous field is by employing technological progress in creating virtual security trainings. When aid workers are operating in volatile environments, providing security trainings face-to-face can be challenging. High costs of production and bad internet connections are referred to as current limitations, but online security trainings are believed to have the potential to reach a broad public in a relatively cheap way in the near future.

Secondly, aid agencies also use humanitarian technologies that were initially employed for reasons of efficiency or effectiveness but had the "fortunate" side effect of protecting staff by limiting their need to be present in the field. Examples of such technologies can be found in technological applications used for needs assessments, goods or services delivery, and monitoring and evaluation (M&E). For instance, tablets and smart phones are used to conduct needs assessments among beneficiaries to make data collection and processing faster and more precise. Although drones in these conflict zones have overly strong military connotations, in the future, some managers hope to use drones for assessing needs and vulnerabilities as drones have a much higher resolution than satellite imagery. Mapping platforms with geo-referenced information can occasionally also be put to use in the assessment of needs. In terms of delivery, cargo drones have been mentioned as a future option, but no respondent mentioned having experience with it. More popularly, virtual cash transfer (e.g., M-Pesa) is being tested and used as a safer and faster option for providing aid than physical commodity distribution. With regard to the distribution of goods, Last Mile Mobile Solutions (LMMS) is an advanced tool to make the "last mile" of distribution more efficient, cheaper, and more dignified. It helps aid agencies

to register beneficiaries, calculate their needs, and fairly distribute the supplies through digitalizing all the information. Beneficiaries receive an ID card, which, upon scanning, can show what they received and what they are entitled to. All this information is also easily accessible in one dataset which simplifies subsequent M&E. Further M&E is often carried out by simply calling beneficiaries or providing phone numbers to recipients. Additionally, staff are asked to make pictures with GPS cameras or to make videos of projects and programs. Somewhat more advanced, satellite imagery is used for M&E purposes. For instance, satellite pictures were used to find out whether shelters were built in a remote and dangerous area in Afghanistan. Given this brief overview of how humanitarian technologies affect aid agency security in volatile settings, we now move on to the propositions and reflect on them by using the interview findings.

Proposition 1a: The use of humanitarian technologies in security management does not reduce risks.

At first sight, there seems to be much to say for this proposition. Often, the core reason for not using certain technological applications was the security risks that the technologies themselves entailed. For instance, basic technologies were not given to local staff in some areas in Somalia and Afghanistan, as armed groups like Al Shabaab in Somalia and the Taliban in Afghanistan oppose such technologies and may harm staff carrying devices. The military roots of these technologies make their use suspicious to armed groups and render local humanitarian staff "legitimate targets." Another example for not using novel technological applications is that the networks on which they rely (e.g., mobile phone networks) are poor or unreliable, such as in South Sudan. With new technologies for security management, security managers therefore identified new security risks, which coincide with Beck's claim that much time is spent on tackling risks that have been introduced by actors themselves.

Pursuing this line of thought, the debate on the security management *of* technologies is worthwhile considering. Respondents shared many security risks warranting careful consideration before introducing technological solutions in response to threats, such as the risk that digital data could be stolen. Also, threat actors use technologies to undermine technologies used in aid agencies' security management:

> However, professional hijackers know by now that organizations equip their cars with [vehicle tracking devices], so they use jamming devices or detection equipment to scan such a car. (Global security manager)

This means that humanitarian actors and malevolent actors enter into a continuing race to outperform each other. In discussions on the security management of technologies, securing the innovations often appeared to become a goal in itself, while the original aim of these technologies (i.e., providing security to staff) seemed lost out of sight and alternative solutions to this initial aim were little debated.

In contrast, however, it is fair to say that not all risks are equal. The use of mobile phone text alerts and Skype in countries like Iraq is perceived to come at little risk to the local staff carrying the necessary devices while risks to international staff are dropping considerably if they do not have to go into the field on a daily or weekly basis. Additionally, the sharing of security information among aid agencies through NGO security fora is another low-risk technology-enabled activity that is likely to considerably reduce risks to staff in the field. In fact, the risks of using these technologies are marginal in comparison to the pre-existing risks to aid agency staff, and thus, some humanitarian technologies appear to enable an actual reduction of security risks.

The proposition can therefore only be partially accepted. Many basic humanitarian technologies can be introduced in aid agency security management to reduce risks to international, national, and local staff. Nevertheless, risks may simply be replaced or even enhanced if armed groups are opposed, networks are unreliable, or malevolent actors develop more advanced technologies.

Proposition 1b: The implementation of humanitarian technologies in security management shifts risks to more vulnerable actors.

Beck's analysis of a link between vulnerability to risks and poverty was by and large reflected in the distribution of risks among aid agency staff. All these technologies enable international and senior national staff to operate from a safe distance. There appears to be little need for them to go into the field themselves and do security assessments, goods distribution, or M&E on the spot. Instead, they are working from a bunkerized or remote location, such as national and regional headquarters, or occasionally even from European cities (e.g., Geneva). For many security managers, the entire process of security information collection, analysis, and dissemination is digitalized. While international and senior national staff work removed from the field in bunkerized or safe spaces, the implications for local staff are context-specific. Their risks may also be decreased by the technology-enabled withdrawal of their colleagues. For instance, threats are sometimes directly aimed at clearly recognizable Western staff which may thereby cause risks indirectly to local staff in their vicinity.

Additionally, local staff are no longer openly and visibly recognizable as associating with Westerners. On the other hand, local staff members are also the only representatives of the aid agency left in the field after the removal of their seniors and may thereby become a target instead. While the context and conditions will thus influence whether individual local staff members are after all better off due to the introduction of humanitarian technologies, it appears undeniable that remaining security risks are directed at local staff.

This is problematic when local staff have little to say over security management decisions. As an exception in this study, local aid workers of one aid agency made their own local risk assessments as well as took their own decisions on whether to continue working:

> We always leave them the freedom to decide for themselves, whether they want to stay on and continue working […] And if they come to the conclusion that they don't, then we will ask them to freeze the operations. (Security manager, Iraq)

Many other security managers, however, answered the question whether local staff could influence security management decisions with silences, sighs, or simple "nos." Although security decisions cannot be directly influenced by local staff in many cases, much local security information comes from local staff in the first place, and through their upward security information provision, local staff can potentially indirectly affect security management decisions.

Thus, the adoption of certain humanitarian technologies for security purposes may not actually shift risks from an international or national staff member to a local staff member, but due to senior staff withdrawal, remaining security risks to agencies are nevertheless directed at local staff. This does not necessarily mean they are at higher risk than before because the implemented technologies may partly reduce their risks (directly or indirectly) as well, but local staff's formal powerlessness over security management decision-making does constitute a matter for concern.

Proposition 2: Humanitarian technology is not a neutral fix for security problems but has political ramifications.

Whereas local staff influence over security management decisions is limited, country directors in turn stress that their operational influence over aid activities is reduced in technology-mediated programs and projects. Thus, even if risks do not shift, some control over resources does shift to local staff members. This may be a great opportunity for capacity-building but, even so, local staff's decisions should not be viewed as neutral or non-political decisions. Since technology-mediated projects are mostly about "relief distributions," local staff are endowed with enormous power as their decisions potentially influence the lives of many beneficiaries to a substantial degree. Certain gatekeepers to local communities may therefore gain significant power if they are the only ones who have digital expertise or when they control the (tele)communication with decision-making staff of aid agencies.

The idea of technological solutions as a neutral fix to humanitarian problems is further challenged by the fact that humanitarian technologies are not simply introduced by aid agencies for objective reasons but that their introduction is likely to be negotiated by actors in the field. As mentioned before, armed groups often oppose technologies, which means that certain devices are not used in areas under the control of these groups. Only one security manager stated that his organization negotiated with an armed group for permission to use GPS cameras:

> They know that if they do not allow us to work with cameras and GPS coordinates and those sort of things (…) we don't work. (Country director, Somalia)

Even when armed groups may be convinced, however, governments may refuse to grant permits or problematize the import of technologies for undisclosed reasons. Additionally, many technologies have military roots and are therefore not yet used in the field as agencies do not want to be associated with international military organizations. Most obviously, drones are so strongly associated with warfighting that they will not be employed in conflict zones. These findings demonstrate that local political conditions influence which technologies are used in the field and that the choice for using humanitarian technologies is therefore not based on an objective assessment by an aid organization.

Thus, the introduction of humanitarian technologies for security reasons is indeed not a neutral fix. It does shift political power to local staff and thus affects local political relations. While, optimistically, this contributes to capacity-building, many international staff members worry about possible misuse of this power. Adding to the idea that humanitarian technologies have political ramifications, there is also a reverse relation: local political dynamics affect the type, speed, and sort of humanitarian technologies introduced in the field as well.

Proposition 3a: Remote Management, as a security strategy, fosters the introduction of humanitarian technologies.

In many dangerous countries, aid agencies follow the textbook example for Remote Management: there are

security reasons for the withdrawal of senior international and national staff, and humanitarian technologies are subsequently introduced to improve the security of local staff as well as to ensure the quality of remotely managed operations. However, the interviews also show another process that leads to the removing of international and national staff, which I label as "accidental Remote Management." In this type of Remote Management, humanitarian technologies simply render it superfluous or unnecessary for senior aid agency staff to go into the volatile field. While many innovative tools may have had non-security purposes initially (e.g., efficiency, effectiveness, cost reduction, more dignified aid provision), they have come to replace "traditional" ways of operating as well as field visits. Unintentionally, such technological applications can therefore contribute to the bunkerization and removing of (inter)national staff. This happens to resonate well with the protection strategies that security managers in unsafe countries widely use, and thus, an aid agency gradually moves into a Remote Management modality.

This finding also hints at the fact that there is a virtuous cycle between Remote Management and humanitarian technology reliance. Whereas Remote Management requires or inspires reliance on technological tools, technologies enable the use or expansion of Remote Management. For example, in remotely managed projects, there is an increased use of information-gathering technologies in the planning phase for needs assessments and finding reliable implementing partners, while monitoring and evaluation activities are also increasingly digitalized. Furthermore, communication technologies are progressively relied on to facilitate interactions between staff members and to relay security information. Next, some agencies stress the importance of resilience when operating in a remote modality, such as the ability to move to cash transfers when paper cash is too dangerous for paying salaries, while others resort to humanitarian technologies in an attempt to regain some control that was lost in going remote. Looking at this as a process, the virtuous cycle between humanitarian technology and Remote Management clearly comes to the surface.

Thus, this proposition holds only partly. Whereas it is indeed true that many aid agencies removed from the field for security reasons and thereafter began to technologize their operations, some agencies end up in remotely managed programs and projects without the intention to do so initially but simply as a result of the lack of perceived need to send seniors into the volatile field when humanitarian technologies are available. Additionally, the proposition can be completed by taking into account the virtuous cycle between humanitarian technologies and Remote Management.

Proposition 3b: Humanitarian technologies distance international and national aid workers from the field.

Respondents report that remotely managed projects, in whatever form, appear to come with a loss of grassroots relations and local knowledge, while the credibility and legitimacy among local staff or beneficiaries is hard to study but often considered to be doubtful at best. As distrust is often voiced with regard to remotely managed projects and discussions quickly shift to formal controls to mitigate adverse effects (e.g., fraud), the emotional or empathetic relation to the field seems to suffer as well. Countering the often-lamented problems of remotely managed projects and programs, one country director based in a bunker in Somalia clarified the importance of his presence in the country while most other country directors were operating from Nairobi, Kenya:

> I am definitely closer to the field than them. It gives me legitimacy when I talk with the high-rank people of the UN. It also gives me some credibility when I talk with the government representatives. […] It's a strong message for the stakeholder that we are working with and also [for] the donors. (Country director, Somalia)

As this quote shows, even the relative proximity of being in an in-country bunker but being able to slightly increase face-to-face contact is preferred to the more distant and more virtualized forms of Remote Management.

On the other hand, with regard to the senior staff's understanding of field conditions, it is worthwhile stressing that humanitarian technologies lead to an improved security information position as well since relevant security data can be gathered faster and more precisely. In addition, advanced analysis capacities provide aid agencies with useful overviews of security and operational trends and developments. Nevertheless, even though this general understanding of security situations may have been improved, it appears that distancing (e.g., in terms of emotions, empathy, legitimacy) is an inevitable effect of reliance on humanitarian technologies. The proposition is therefore supported.

Discussion

In this paper, I have attempted to bridge the gap between, on the one hand, practice-based studies on technological opportunities for aid agency security management, and, on the other hand, fundamental explanations of aid agency insecurity and technology-enabled distancing. Apart from bridging this epistemic gap (see Fast 2010), the findings clearly bring to the fore a more balanced perspective with regard to the merits and risks

of humanitarian technologies for security management than are often published. By means of the empirical analyses for each proposition, I will discuss the implications of my findings for the literature.

Based on the interviews, I found that every technology employed in security management introduces new risks. These risks may result from usage of these technologies (e.g., armed groups threaten aid workers carrying mobile phones) or from the potential undermining of the technology (e.g., malevolent actors may jam vehicle-tracking devices). Nevertheless, the overall security risks to aid workers is perceived to be much lower after the introduction of humanitarian technologies than before in many contexts, because security information is more easily collected and disseminated and staff are less exposed. The focus of security managers therefore easily shifts to the security management *of* these technologies (see e.g., Byrne 2016; Sandvik et al. 2014; Vitaliev 2009). Even though this may overlook the fact that technologies are fundamentally insecure (Beck 1992; Sandvik 2016), it would be misguided to believe that overall risks are not reduced by humanitarian technology use in aid agency security management.

A worrying counter-argument would be that risks are shifted towards the more vulnerable actors, in this case local aid workers. The idea of shifting risks appears too simplistic as the same technologies that enabled senior staff to withdraw from the field may also reduce risks to local aid workers. On the other hand, local staff members are frequently the only aid agency's employees still facing considerable work-related risks which renders their minimal influence over security management decisions in many agencies concerning. The attraction between a marginalized position and risk vulnerability, as predicted by Beck (1992), is therefore ambiguous. Relatively speaking, local staff face a higher exposure than those that are not bunkerized (see Simpson 2015; Egeland et al. 2011:25; Stoddard et al. 2009), but in absolute terms, local staff may still be better off after the implementation of humanitarian technologies in security management.

Next, I find evidence for the idea that the introduction of humanitarian technologies translates into a shift of power to local staff members and a potential restructuring of local political relations. This is not problematic per se, because it also provides an opportunity for local staff members to develop their capacities and grow more independent. However, country directors and security managers alike worry about power misuse. Additionally, it is worthwhile realizing that the aid agency is not independently and objectively deciding which technologies are implemented. Instead, local politics bears heavily on if and how innovative tools can be used in the field. For example, armed groups veto technologies that can be used for military purposes and governments complicate the use of certain tools for their own reasons. While the influence of humanitarian technologies on local political power relations may not come as a surprise (Jacobsen 2015; Sandstrom 2014; Sandvik et al. 2014), the reverse influence has been ignored, even though it fits the idea that local actors can be expected to be active negotiators in the political arenas in which humanitarian action takes place (see Hilhorst and Jansen 2010).

Furthermore, the link between Remote Management and technology use is clear and undeniable. I find that many agencies withdrew from unsafe areas for security reasons and are now resorting to technologies in order to enhance their control over projects and programs. However, there is also an alternative process for going remote though. Some agencies introduced humanitarian technologies for the sake of efficiency, effectiveness, or recipient dignity, with as a beneficial side-effect that senior staff could be removed to safer places. This "accidental Remote Management" subsequently inspires the introduction of new humanitarian technologies, and thus, a virtuous cycle between Remote Management and technology use ensues. Others have found a link between Remote Management and the use of humanitarian technologies before but generally viewed technologies as a result of Remote Management (see Andersson and Weigand 2015; Collinson and Duffield 2014), while the interviews indicate the possibility of a reverse pathway as well. Donini And Maxwell (2013: 413) raised the question "[Are] remote technologies partly what drive the tendency towards the increasing remoteness of humanitarian management, or is the development of such technology merely a means of coping with a deteriorating security and access situation?" In response, I thus conclude that many aid agencies employ technologies to cope with operating from a distance but that there is also "accidental Remote Management" in which remote technologies result in staff withdrawal.

Lastly, technology-enabled Remote Management may be based on better situational and security information and analysis, but the distance between senior staff and local staff members is considerable. The specific local situation is less-understood, emotional and empathetic involvement suffers, and the credibility and legitimacy of agencies declines. This is in line with critical scholars' criticism that there is a gap in grassroot relations and knowledge as well as a growing social and existential distance from the field (e.g., Duffield 2012; Donini and Maxwell 2013; Sandvik 2016). New technologies are constantly adopted and implemented to overcome the virtual gaps but fail to do so (see Andersson and Weigand 2015). While not tested in this study, the growing distance appears to render reality even more threatening to aid workers, thus leaving aid agencies "trapped"

in a problematic implementation modality (Donini and Maxwell 2013), as evidenced by the firm belief of many security managers that they would not operate in many regions for the foreseeable future.

Conclusion

Aid agencies in some of the most dangerous countries report their use of a variety of humanitarian technologies that contribute to their security management. The findings on the processes and consequences of using technology for aid interventions corroborate, refine, and add to more fundamental research on trends in the aid sector, thereby bridging the epistemic gap to practice-based reports (Fast 2010). Contributing to the "critical scholarly engagement with the humanitarian turn to technology" (Sandvik et al. 2014:222), my findings are threefold. Firstly, I find that humanitarian technologies, dependent on the context and conditions, mitigate risks to international, national, and local aid workers, while remaining risks are unequally directed at relatively powerless local staff members. Secondly, the idea that technology is a neutral solution to problems is dispelled by reference to the local political origins and consequences of technology use. Thirdly, I argue that there is a virtuous cycle between the introduction of technological tools and the (accidental) distancing of international and national staff, rendering the latter socially removed from their local counterparts and beneficiaries.

From a practical point of view, this study shows that reliance on humanitarian technologies in unsafe areas is not necessarily as problematic as the critical literature often suggests. Aid agencies can therefore adopt and implement humanitarian technologies for security management without necessarily harming their humanitarian endeavors. For optimal consequences, pre-implementation assessments should focus on the effects on risks to local staff members, the influence on local political relations, and the long-term relations to beneficiaries. An additional practical conclusion of this research is that, when specific humanitarian technologies reduce senior staff presence in the field, agencies would do well to give local staff a bigger voice in (individual) security management decisions.

This study also has several limitations which are worthwhile addressing in future research. Firstly, this study is limited to analysis on the basis of interviews with senior international staff members of aid agencies. Ethnographic or observational research could add to these formal discursive reflections by studying how security managers and country directors act towards and informally talk about technology and the implications of it. Furthermore, it is essential to interview local staff members and beneficiaries in future research to get a more comprehensive understanding of how they perceive their risks after the withdrawal of senior staff, how they negotiate which humanitarian technologies are introduced, and how these tools affect community relations. Next, although respondents were asked to reflect on their earlier experiences with technology use and Remote Management as well as to describe the process of withdrawing from the field, ethnographic research or a process-based analysis of documents would help to create a better understanding of the interaction between technology use and Remote Management and could for instance dissect more specifically how accidental Remote Management takes place. By extension, and highly relevant from a practical point of view, it would be interesting to study which assessments aid agencies conducted before implementing certain humanitarian technologies and to subsequently research the consequences of these humanitarian technologies. This analysis may indicate how pre-implementation assessments can mitigate potentially adverse effects, while it may also reveal whether some of the negative appraisals of humanitarian technologies in the critical literature can partly be attributed to insufficient preparation before implementation.

The fact that technology-based Remote Management appears an unstoppable trend (Collinson and Duffield 2013) makes it all the more important for humanitarian managers to know "what exactly they are buying into" (Duffield 2013:23). We may therefore conclude with Donini and Maxwell (2013:412–413) that the "future of humanitarian action as a compassionate endeavour is likely to hinge on its ability to maintain a critical balance between the promise of technology and the reality of peoples' lives on the ground."

Endnotes

[1]https://aidworkersecurity.org/incidents/report/country.

Appendix 1

In advance of the interviews, questions were adjusted to the type of organization (NGO, UN, ICRC), country of operations, and the role of the respondent (e.g., security manager, country director).

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?

Abbreviations
ICRC: International Committee of the Red Cross; IFRC: International Federation of the Red Cross; ISIL: Islamic State of Iraq and the Levant; M&E: Monitoring and evaluation; NGOs: Non-governmental organizations; UN: United Nations

Acknowledgements
The author wishes to thank Bram Jansen for his inspiring supervision and continued encouragement. In addition, the author expresses his gratitude to the editor and two anonymous reviewers for their thorough reviews and helpful comments. The author, lastly, wants to thank the respondents of this study, many of which work in volatile countries and are confronted with complicated security dilemmas.

Funding
Not applicable.

Availability of data and materials
The author promised the respondents that data would not be shared.

Author's information
Jori Pascal Kalkman is a PhD student at the Vrije University Amsterdam, the Netherlands Defense Academy, and TNO. This article is based on the author's master thesis at the Wageningen University which was graded cum laude.

Competing interests
The author declares no competing interests.

Publisher's Note

Author details
[1]Department of Organization Sciences, VU University, De Boelelaan 1105, 1081HV Amsterdam, The Netherlands. [2]Department of Management, Organisation and Defence Economics, Netherlands Defence Academy, De la Reyweg 120, 4818BB Breda, The Netherlands. [3]Defence, Safety and Security, TNO, P.O. Box 23, 3769ZG Soesterberg, The Netherlands.

Received: 6 October 2017 Accepted: 2 January 2018
Published online: 11 January 2018

References

Abdelnour S, Saeed AM (2014) Technologizing humanitarian space: Darfur advocacy and the rape-stove panacea. Int Political Sociol 8:145–163
Abild E (2010) Creating humanitarian space: a case study of Somalia. Refug Surv Q 29:67–102
Andersson R, Weigand F (2015) Intervention at risk: the vicious cycle of distance and danger in Mali and Afghanistan. J Interv Statehood 9(4):519–541
Beck U (1992) Risk society: towards a new modernity. Sage Publications, London
Beck U (2006) Living in the world risk society. Econ Soc 35:329–345
Byrne R (2016) Trends in intelligence gathering by governments. In: Vazquez Llorente R, Wall I (eds.) Communications technology and humanitarian delivery: challenges and opportunities for security risk management. European Interagency Security Forum (EISF)
Canter DV, Sarangi S (2009) The rhetorical foundation of militant jihad. In: Canter DV (ed) Faces of terrorism: multidisciplinary perspectives. Wiley-Blackwell, Chihester
Carle A, Chkam H (2006) Humanitarian action in the new security environment: policy and operational implications in Iraq. HPG background paper, London
Cater J (2011) Skype: a cost effective method for qualitative research. Rehabilitation Couns Educ J 4(2):3–4
Collinson S, Duffield M (2013) Paradoxes of presence: risk management and aid culture in challenging environments. Humanitarian Policy Group, London
Cunningham AJ (2017) Kidnapping and the limits of acceptance. J Int Humanit Action 2:4
De Palacios G (2016) Applicability of open source systems (Ushahidi) for security management, incident and crisis mapping: Accion contra el Hambre (ACF-Spain) case study. In: Vazquez Llorente R, Wall I (eds.) Communications technology and humanitarian delivery: challenges and opportunities for security risk management. European Interagency Security Forum (EISF)
Deakin H, Wakefield K (2014) Skype interviewing: reflections of two PhD researchers. Qual Res 14(5):603–616
Donini A, 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. Int Rev Red Cross 95(890):384–413
Duffield M (2010) Risk-management and the fortified aid compound: everyday life in post-interventionary society. J Interv Statehood 4(4):453–474
Duffield M (2012) Challenging environments: danger, resilience and the aid industry. Secur Dialogue 43:475–492
Duffield M (2013) Disaster-resilience in the network age access-denial and the rise of cyber-humanitarianism. DIIS Working Paper 2013:23
Duffield M (2014) From immersion to simulation: remote methodologies and the decline of area studies. Rev Afr Polit Econ 41(sup 1):S75–S94
Duffield M (2016) The resilience of the ruins: towards a critique of digital humanitarianism. Resilience 4(3):147–165
Egeland J, Harmer A, Stoddard A (2011) To stay and deliver. Good practice for humanitarians in complex security environments. OCHA: Policy and Studies Series

Fast LA (2010) Mind the gap: documenting and explaining violence against aid workers. European J Int Relat 16:365–389
Fast LA, Freeman CF, O'Neill M, Rowley E (2013) In acceptance we trust? Conceptualising acceptance as a viable approach to NGO security management. Disasters 37(2):222–243
Fuji LA (2009) Interpreting truth and lies in stories of conflict and violence. In: Sriram CL, King JC, Mertus JA, Martin-Ortega O, Herman J (eds.) Surviving Field Research: working in violent and difficult situations. Routledge, New York.
Gonsalves A (2016) Applying serious gaming to humanitarian security: a framework for mixed-reality training. In: Vazquez Llorente R, Wall I (eds.) Communications technology and humanitarian delivery: challenges and opportunities for security risk management. European Interagency Security Forum (EISF)
Gundel J (2006) Humanitarian action in the new security environment: policy and operational implications in Somalia and Somaliland. HPG Background Paper
Hilhorst D, Jansen BJ (2010) Humanitarian space as arena: a perspective on the everyday politics of aid. Dev Chang 41(6):1117–1139
HPN (2010) Operational security management in violent environments. Good practice review: number 8. Humanitarian Practice Network, London
IFRC (2013) World disaster report 2013, focus on technology and the future of humanitarian action. International Foundation of the Red Cross and Red Crescent, Geneva
Jacobsen KL (2015) The politics of humanitarian technology: good intentions, unintended consequences and insecurity. Routledge, New York
Janghorban R, Roudsari RL, Taghipour A (2014) Skype interviewing: the new generation of online synchronous interview in qualitative research. Int J Qual Stud Health Well-Being 9:1
Karlsrud J, Rosén F (2013) In the eye of the beholder? UN and the use of drones to protect civilians. Stab Int J Sec Dev 2:2
Mayo A (2016) SMS technology and bulk SMS delivery systems: their role in security management for the humanitarian community. In: Vazquez Llorente R, Wall I (eds.) Communications technology and humanitarian delivery: challenges and opportunities for security risk management. European Interagency Security Forum (EISF)
Meier P (2011) New information technologies and their impact on the humanitarian sector. Int. Rev Red Cross 93(884):1239–1263
Miles MB, Huberman AM, Saldaña J (2013) Qualitative data analysis: a methods sourcebook, 3rd edn. Sage Publications, London
Powell C (2001) Remarks to the National Foreign Policy Conference for leaders of nongovernmental organizations. http://avalon.law.yale.edu/sept11/powell_brief31.asp. Accessed 27 Sept 2017.
Qadir J, Ali A, ru Rasool R, Zwitter A, Sathiaseelan A, Crowcroft J (2016) Crisis analytics: big data-driven crisis response. J Int Humanit Action 1:12
Sandstrom K (2014) Remoteness and 'demonitored space' in Afghanistan. Peacebuilding 2(3):286-302. Sage Publications, London
Sandvik KB (2016) The humanitarian cyberspace: shrinking space or an expanding frontier? Third World Q 37(1):17–32
Sandvik KB (2017) Now is the time to deliver: looking for humanitarian innovation's theory of change. J Int Humanit Action 2:8
Sandvik KB, Jumbert MG, Karlsrud J, Kaufmann M (2014) Humanitarian technology: a critical research agenda. Int Rev Red Cross 96(893):219–242
Sandvik KB, Lohne K (2014) The rise of the humanitarian drone: giving content to an emerging concept. Millennium: J Int Stud 43(1):145-164
Schneiker A (2013) The vulnerable do-gooders: security strategies of German aid agencies. Disasters 37(2):244–266
Sheik M, Gutierrez MI, Bolton P, Spiegel P, Thieren M, Burnham G (2000) Deaths among humanitarian workers. Br Med J 321:166–168
Simpson J (2015) Risk management responses to armed non-state actor risk in Afghanistan. Int Rev Soc Res 5(3):156–166
Steets J, Reichhold U, Sagmeister E (2012) Evaluation and review of humanitarian access strategies in DG ECHO funded interventions. Global Public Policy Institute: ECHO report
Stoddard A, Harmer A, Czwarno M (2017) Aid Worker Security Report 2017: Behind the attacks: a look at the perpetrators of violence against aid workers. Humanitarian Outcomes
Stoddard A, Harmer A, V DiDomenico (2009) Providing aid in insecure environments: 2009 update trends in violence against aid workers and the operational response. HPG Policy Brief 34
Stoddard A, Harmer A, Renouf JS (2010). Once removed: lessons and challenges in remote management of humanitarian operations for insecure areas. Humanitarian Outcomes
UNOCHA (2013) Humanitarianism in the network age. United Nations, New York
van der Windt P, Humphreys M (2016) Crowdseeding conflict data. J Confl Resolut 60(4):748–781
Vazquez Llorente R, Wall I (eds.) (2016) Communications technology and humanitarian delivery: challenges and opportunities for security risk management. European Interagency Security Forum (EISF)
Vitaliev D (2009) Cyber security for international aid agencies: a primer. SMI Professional Development Brief 3