The Duties of an NGO Security Advisor

Emmanuelle Strub

Former Security Advisor, Médecins du Monde France; es@actarisk.com
Translated by Nina Friedman

Abstract

A security advisor for Médecins du Monde France between 2012 and 2016, Emmanuelle Strub recalls her experience and some of the major shifts in risk management in the NGO sector in recent years. In particular, at a time of global normalisation of the aid sector, she describes her own efforts to streamline security management in her organisation: empowering field teams and, in particular, heads of mission, emphasising the crucial role of obtaining consent from the various stakeholders in the countries of intervention, and developing security trainings, crisis-management tools and a risk-management methodology. Yet, she warns, the trend today, with the advent of the duty-of-care concept, is to shift the use of risk management from enabling operations and facilitating access to populations to protecting the organisation from legal or reputational risks.

Keywords: risk management, security, duty of care, MdM

History

Security-risk management has long been a concern at Médecins du Monde (MdM), as it was for other humanitarian agencies operating at the height of the Cold War. However, it was in the 1990s that security had to address its own set of issues. The collapse of the Soviet bloc and the post-Cold War conflicts created safety issues for humanitarian agencies: a booming aid sector led to an increase in exposure, together with a trend for humanitarian organisations to shift from working on the periphery of conflicts to the heart of them. Yugoslavia, Chechnya, Rwanda and the entire Great Lakes region of Africa became particularly high-risk areas for aid workers.

It was during the intervention in Somalia in 1992 that the interface between security, operational procedures and humanitarian principles became central for MdM. The political and security climate at the time confined NGOs to urban centres across Somalia, while the looting of humanitarian convoys by armed men on the main roads made regular aid delivery to the IDP (internally displaced person) camps difficult. Was armed protection necessary to ensure access to vulnerable populations? Five years later, in 1997, three MdM-Spain volunteers were killed and a fourth wounded in a targeted attack in Ruhengeri, Northern Rwanda. In Chechnya and the former Yugoslavia, NGO personnel were being kidnapped or targeted. Those incidents made security a tangible issue for MdM, setting off an internal debate about individual versus institutional prerogatives. Who was responsible for what in terms of security? Who was authorised to make decisions, and based on what information?

To answer those questions, a 'security module' was incorporated into departure preparations for international volunteers, and the first security booklet was developed. The module and the booklet explained the risks that volunteers might face, measures to reduce them, responsibilities and procedures for sharing security information within projects and the organisation as a whole, and rules for behaviour. During that same period, in the late 1990s, the first country-specific security plans were drawn up; with each violent incident affecting the organisation and other humanitarian actors, security management took shape.

Compared to other humanitarian agencies, MdM was more or less spared in terms of direct incidents, but in October 2006 the international operations director instigated the creation of a position devoted to integrating security into the structure of the organisation. Drawing on his experience as Bernard Kouchner's special advisor in Kosovo and other positions, the international operations director was convinced that security required clear and harmonised procedures, just like logistics or finance, and someone with technical expertise in charge. Some on the Board of Directors (the decision-making body at MdM) advised against the creation of the position, in the belief that relying on local expertise was preferable and fearing that an outsider's

Journal of Humanitarian Affairs Volume 1, No. 2 (2019), 32–37 © The authors
http://dx.doi.org/10.7227/JHA.015

MANCHESTER 1824
Manchester University Press

security assessments would threaten the existence of the programmes. Three people would hold the position of security advisor in turn before I took it six years later, in February 2012.

The position had been vacant for nearly a year. The human resources department had struggled to find suitable candidates, probably because this was a new position in the NGO sector and there were few specialists. They interviewed two people with security experience in the private sector and the military; my curriculum vitae did not interest them at first. My standard humanitarian career path in NGOs and international organisations meant I had only a few months' experience in that type of position. However, my 2002 Master's *memoire* on aid workers' security in Afghanistan ('Quelle place pour la compréhension dans la trilogie: acceptabilité, protection et dissuasion?'[1]) gave me the justification I needed to apply. I ultimately got an interview, after resubmitting my application and calling a few people I knew at MdM.

When I started, my job description was as follows: monitor the risks and threats to project teams in countries where MdM was working; provide methodological and technical support for writing, finalising and setting up security-management documents at the missions; monitor the implementation of security analysis and management tools at international programmes and prepare a periodic report for the International Operations Directorate; advise the project teams on managing security incidents and update the security-incident database; support security-management briefings for field teams; and maintain the existing security network and take part in outside meetings. It was a sizeable challenge, given that in 2012 MdM had a presence on every continent, in some forty countries, with 136 international and 1,700 national employees. At headquarters they had fourteen desk managers to oversee the sixty-five projects.

In addition, I was unclear about my role. I had practically no support, though the scope of my job was enormous, from strengthening the overall security framework to providing operational support at one of multiple field projects. What was expected of me? Technical support? Context analysis? Alerts? Operational, strategic and decision-making advice? Or simply reviewing the security plans produced? It seemed like I had as many roles as interlocutors, each with their own idea of what a security advisor should do. Several tools had been put in place between 2006 and 2012: security documentation for each mission, called a 'security plan', which summarised the context, risks to personnel and operations, security measures and contingency plans for a possible evacuation or lockdown situation; a one- to two-hour awareness-raising session on security for all volunteers leaving on mission during their departure preparation; and, most importantly, a kidnapping risk-management policy. That policy was designed and put in place after two expatriates were abducted in Somalia in the fall of 2008. It required identifying the kidnapping risk in each intervention zone; a specific briefing for people heading to high- and very high-risk areas about the risk and the means being used to reduce it; and confidentially obtaining and managing proof of identity. The idea was not just to better prepare for managing a kidnapping but also to clearly inform volunteers that the risk existed.

The resources available when I took the position in early 2012 had not changed since the position was created in 2006. There was one person positioned in the technical support and advocacy department – a department that consisted of about a dozen, mainly medical, technical advisors. And while the department was part of the International Operations Directorate, the relationship with operational managers from headquarters and the field was functional, not hierarchical.

Security Advisor, 2012–16

Task One: Training the Heads of Mission

Two months after I started as MdM's security advisor I travelled to Yemen, Afghanistan and Pakistan. I discovered very different security practices and cultures, reflecting the experience of each head of mission. There was no MdM 'security method'. Different heads of mission used different tools and had different security rules and levels of risk-taking. In Kabul, some of the expats would go jogging in a nearby park, while in Islamabad even walking on the street was prohibited. Each team's perception of security reflected the views of whoever was head of mission at the time. The heads of mission in Yemen and Pakistan were very experienced but had different backgrounds and views. For the teams in Afghanistan – specialists in risk reduction for drug users, with no experience in a war context – the context was so complex that luck was the only thing that mattered when it came to security management. The MdM logo was the only reminder that the teams in the three missions worked for the same organisation.

My first task in standardising practices and strengthening the overall security-management framework within the organisation was to create an annual training for heads of mission and programme managers. The training had three goals: ensure a common understanding of security-related terms (What is a threat? And a risk? What do we mean by acceptance strategy? Protection? Deterrence?), learn when and how to use the tools (Which tool should be used to analyse the risks? What should go into a security plan? How should an incident

be reported?) and know how to react in case of a serious incident (When and how should we prepare an evacuation or lockdown plan? What should we do in case of a serious accident, kidnapping or sexual assault?).

I also had to 'operationalise' the organisation's security mantras: 'MdM favours acceptance' and 'security is everyone's responsibility'. *Acceptance* was rightly understood in terms of how the organisation and its programmes were perceived by the population and authorities. Yet 'acceptance is founded on effective relationships and cultivating and maintaining consent from beneficiaries, local authorities, belligerents and other stakeholders' (Fast and O'Neill, 2010). And building such relationships requires not only time but human resources with interpersonal, communication and negotiation skills. Although those annual security trainings were an opportunity to remind colleagues that implementing an acceptance strategy required budgeting and planning, only once in five years was I able to train operations managers in headquarters on negotiating access.

'Security is everyone's responsibility' was another mantra at departure-preparation awareness-raising sessions. If everyone was responsible for their own behaviour and for understanding and respecting the rules, then clearly defining the responsibilities of each position was essential. Security-management training helped spell out security management and place it in the hands of the head of mission or base manager. The commonly accepted idea at the time was that security was the logistician's responsibility. The logistics department makes an essential contribution to security management by managing the vehicle pool, the buildings and the means of communication used by guards and drivers. However, logisticians are not trained to analyse risk or develop an acceptance strategy. While some of them do it, the negotiation skills needed to set up operations and analysis, and written and oral communication skills, are not in the logistician's job description. In addition, since the heads of mission are ultimately responsible for the safety of their employees and operations, I felt it essential that they be trained and be able to delegate some of the tasks, if necessary, to competent people on their teams.

Those trainings were also an opportunity to remind people of security management's only two objectives: to improve safety for both international and national staff and to increase our operational capacity. Those objectives were also the subject of my first message to the Board of Directors six months after I started, as were the resources needed to develop and standardise our risk-analysis and management tools, to train the staff in their use and to enhance our organisational capacity to deal with a serious incident.

That last point was the hardest to achieve, because it required directorate involvement. While everyone agreed in principle that it is essential to prepare for managing a crisis, when it came time to do it, no one was available. It wasn't until 2013, when two ACTED employees were kidnapped in an area of Syria where we were also present, that the directorate and Board of Directors met to set up a crisis unit.

Task Two: Developing a Risk-Management Methodology for the Field

From 2012, I organised one-day risk-analysis workshops during each of my visits (be it Colombia, Myanmar, Algeria, the Sahel or the Democratic Republic of Congo), with all of the team members – from the head of mission to support staff. I wanted to make sure the teams had a shared view of the context and of the risks taken by the organisation and by each of them, according to their individual profile (gender, nationality, ethnicity and position in the organisation). The workshops also helped develop a common language when talking about threat, vulnerability and risk, and created a space for the staff to share their own perceptions of the dangers they and the organisation faced. Using a risk-analysis tool and methodology, we were able to check those perceptions against the facts. The workshops helped to set up risk-reduction measures for all to follow but also to get rid of inadequate safety rules that put into question the validity of the whole security plan. In most cases, those rules had to do with the personal lives of international staff, limiting their movements. The prohibitions against being out and about at such and such a time, in such and such a place, alone or not, were sometimes relaxed because they were useless. We agreed that the risk of having one's bag stolen while walking down the street was a risk that could be taken, and that it was counterproductive to prohibit being out and about for that. The lifting of the restriction was of course accompanied by awareness training regarding the risk, as well as a reminder about how to be mindful of one's surroundings and personal effects and to be unobtrusive and non-ostentatious.

The discussions about individual perceptions of risk led to the issue of the relationship between gender and safety. Do women face different risks from men? Do gender-specific risks justify imposing strict rules for women alone? The answers to those questions in some of our security manuals meant that, for example, 'a female expat should not go out unless accompanied by a male colleague' in situations that did not seem to justify it in any way. However, the biggest problem was the failure to report incidents of sexual assault against female staff (mostly national staff), even verbally.

Task Three: Crisis Management

The effectiveness of crisis-management training became clear on my first visit to Yemen. The day before I

returned to Paris, two members of our national staff were kidnapped while driving from Sa'dah to Sana'a. The head of mission had recently attended kidnapping-management training in Yemen. The key elements of crisis management were thus fresh in his mind (informing the families, managing the media, maintaining confidentiality, etc.), and the list of key contacts was up-to-date. As a result, he was immediately able to send the kidnappers a consistent message, inform the families, reach out to organisations with experience in similar situations and contact the governor of the province to request his intervention. Both victims were released that same evening. A few days later we got the vehicle back, too. All that without giving anything in exchange.

The response to the incident in Yemen was exceptional. In most of my field visits, colleagues expressed their concerns about our headquarters' ability to respond to a serious incident in the absence of an institutional risk-management policy and a standardised approach to security management. 'What will headquarters do if we have a problem? Who should I call first? You? My desk officer? The embassy? The police? The security guard whose cousin works in security services?' It wasn't until late 2013 that the Board of Directors signed off a crisis-management protocol and I was able to provide clear answers to those questions.

However, I did not wait until 2013 to start training the heads of mission in how to manage serious incidents. The aim was to help them know what to do without relying exclusively on support and guidance from headquarters, which would arrive late if at all. At the end of the day, the heads of mission and field coordinators would be on the front line, and it would be up to them to make the initial decisions. I relied on the EISF (European Interagency Security Forum) network to set up the crisis-management trainings for all the heads of mission. We held several crisis-management trainings in the Sahel, Turkey, Thailand and Kenya. Most MdM heads of mission completed the training between 2013 and 2015.

Task Four: Simplifying the Security Tools

The EISF network and the humanitarian security literature it curates also helped guide my thinking and practice regarding risk management. It was an indispensable resource when I decided to standardise the tools being used. Which tool to choose? Which format for which use? To answer these questions, I also sought the opinion of my MdM colleagues. I requested that a security steering committee be created within the International Operations Directorate to exchange information on standardising security management. I did not get the resources to set up the committee, so I made the changes myself, with inputs from other humanitarian security professionals outside the organisation.

I used the 'less is more' principle when revising the tools. It seemed essential to reduce the size of the security plans to make them readable and thus functional and useful. Security plans from the 2000s were often fifty-page-long documents (excluding appendices) and rarely read or updated, since those tasks seemed massive. In addition, I simplified the risk-analysis tools, eliminating dozens of indicators, made incident reporting meaningful and established routine briefings for people arriving at the mission. I ended the colour-coded security-level system – useful for very large organisations that need to communicate changes in the situation and the rules to staff and their families – as it gave no information about the threats, nor was it flexible enough for an organisation like MdM. I continued to use a colour code in the overview, like the one used by the French Ministry of Foreign Affairs in the maps of its *Advice to Travellers* section, for internal communication purposes only.

My first priority was to advocate for more human resources for context monitoring, operational support and training for all personnel. That strategy may have paid off, since in late 2016, after I left, I was replaced by a three-person security department reporting directly to the International Operations Directorate and supported by regional security advisors.

Task Five: Security-Incident Analysis

The analysis of security incidents in the field also needed to improve. In 2012, it was impossible to know what type of incidents had the most impact on our field staff. Was it true, as everyone said, that road accidents were the leading cause of death among aid workers? While that was probably true in the 1990s, the logistical management of vehicle pools, driver training and respect for traffic rules (speed, seatbelts and car maintenance) had improved, as the 'Aid Worker Security Database' (Humanitarian Outcomes, n.d.) demonstrated. Moreover, I found only a few car accidents in our archives, though it was likely that not all the incidents had been reported.

In fact, one of the biggest obstacles to incident reporting was the fear of consequences and of headquarters interfering in the mission's affairs. Thanks to the training and field visits, the heads of mission were more willing to report incidents, making the global analysis more accurate. It turned out that traffic accidents were in fact very rare, and that verbal and written threats and threatening gestures were the leading cause of incidents and source of stress for the staff. Reporting incidents – that is, real examples – to headquarters also helped to communicate the need for additional precaution. For example, a low-quality gas bottle carelessly transported in the back of a pickup, which exploded, injuring the driver and his passenger, and a refrigerator that caught fire, setting the living

quarters ablaze, offered opportunities to discuss the need to check gas and electric equipment and to equip offices and living quarters with fire extinguishers.

At the same time, I tried to get an overview of the situation at each context of intervention. I did the security briefing for each head of mission, and I had to be up-to-date on the context and the risks people would face. I then hired a private security company (Scutum Security First), which sent me situation updates on incidents in countries where MdM was present, roughly ten-line summaries of the situation shared within an hour of the incident. The updates did not change how we did things, as the field teams often got real-time information through their own networks. But they allowed for a critical reading of the analyses produced by the field, reducing the risk of being caught off-guard if the incident had repercussions for our teams or operations.

Challenges

NGO Internal Risk-Analysis Capacity

Given the abundance of information and analysis produced by the security company, the United Nations Department of Safety and Security (UNDSS), various think tanks, like the International Crisis Group (ICG), and Integrated Regional Information Networks (IRIN, now The New Humanitarian), it was a challenge for the field teams to maintain their own analysis capacity based on diverse, reliable information sources. The emergence of NGOs specialising in security-information analysis and management for humanitarian organisations, such as INSO (International NGO Safety Organisation), had undermined the organisation's in-house capabilities. INSO provides security information, analysis, recommendations and sometimes training in the contexts where it has a presence. Thus, in some countries, MdM tended to rely on INSO's analysis and recommendations rather than its own resources, making it less capable of developing its own network of contacts and more dependent on decisions made by others. It seemed essential to me that an organisation like MdM maintained its analysis capacity, so that it could make its own decisions based on its own analysis, even when that analysis contradicted that of INSO or UNDSS.

Remote Management

Developing our own operational skills was also essential. From 2012 to 2016, we had to resort to so-called 'remote' operations in places where part of the team could not go for security reasons. This was not a new operating mode. We had already used it in Iraq and Mali, but its use in Syria forced us to consider all its constraints: the size of the operations, the risks run by the employees on the ground and the need to address questions of corruption and operational compromises.

At MdM, it took some time to agree what the term 'remote' meant, since some felt that once employees paid directly by MdM were in the field, we were directly managing operations. Yet the central point of 'remote management' is that, for security reasons, the decision-maker (programme manager, base manager or head of mission) is far away from the field project. In the case of our Syria operations, the decision-makers were all expatriates who had to leave Syria in 2013 due to the high risk of kidnapping. The national staff, recruited locally the previous year, remained in place to work in the medical facilities or manage the drug supply, and had to deal with bombings and other conflict-related risks. The national staff were also refugees, finding themselves wearing two hats – as NGO workers and directly affected by the conflict – and having to deal with the pressures that go with both. The other challenge was monitoring the quality of the services offered and the impartiality with which they were being provided – monitoring that required resources and a new type of arrangement.

Duty of Care

From 2012 to 2016, security management also incorporated a legal dimension, as the organisation could be held liable if an incident harmed an employee. . The question of legal risk came up at MdM in July 2010, thanks to enactment of the External Action of the State law and the map of officially discouraged red zones. That law enabled lawsuits against NGOs entering red zones if they fell victim to an incident requiring government intervention. In 2011, a Samaritan's Purse employee sued her organisation in the United States after being kidnapped in Darfur the previous year. The first such case in Europe happened in 2015, when Steve Dennis sued the Norwegian Refugee Council after he was kidnapped in Kenya. In France, the Karachi case (an attack in which Naval Group employees were killed) demonstrated the potential legal risk from criminal or terrorist actions. The courts stated that Naval Group should have anticipated the risk and taken appropriate measures to ensure that the attack did not happen:

> By virtue of the employment contract between it and its employee, the employer has a duty of care toward the latter, in particular with regard to occupational accidents, the failure of that duty having the character of an inexcusable fault as defined by Article L452-1 of the Social Security Code, when the employer was, or should have been, aware of the danger to which the employee was exposed and failed to take the necessary measures to protect him from it.
>
> (Cour d'appel, Paris, 2018)

Duty of care caused security management to shift its focus from the security of operations and people to the security of the organisation. The 'duty of care' approach to security would stress the need for security procedures at all levels of the organisation, make security training routine via online training courses, standardise security measures according to a level-of-risk assessment and tend to avoid risk in order to avoid situations where 'the employer was, or should have been, aware of the danger to which the employee was exposed and failed to take the necessary measures to protect him from it'.

Institutional donors would also start using the existence of security documents, standardised procedures and approved 'security' posts in the field as an indicator of good management. Donors do not have the means to ensure that an organisation is capable of properly analysing the contexts in which it intervenes or has a real risk-management strategy and not just a policy of risk avoidance.

Note

1 Translation: What role can understanding play in the acceptability-deterrence-protection triangle?.

Bibliography

Cour d'appel, Paris (2018), n° 15/10172, 13 April, www.institut-numerique.org/section-1-la-jurisprudence-karachi-apparition-du-risque-juridique-en-matiere-de-violences-criminelles-a-lencontre-des-expatries-52a97c046b16f (accessed 16 July 2019).

Fast, L. and O'Neill, M. (2010), 'A Closer Look at Acceptance', *Humanitarian Exchange Magazine*, 47, 5–6.

Humanitarian Outcomes (n.d.), 'The Aid Worker Security Database', https://aidworkersecurity.org/ (accessed 12 June 2019).