



VERBAND
ENTWICKLUNGSPOLITIK
DEUTSCHER
NICHT-
REGIERUNGS-
ORGANISATIONEN E.V.

ASSOCIATION
OF GERMAN
DEVELOPMENT
NGO'S



Minimum Standards regarding Staff Security in Humanitarian Aid

Contents

Foreword	2
1. Introduction	3
2. Overview of the level of debate on the topic	5
2.1 The position of the UN and international aid organisations	5
2.2 The status of debate in Germany.....	5
3. Improving security management in an organisation	7
3.1 Mainstreaming the topic within an organisation	7
3.2 Working out a »security policy« tailored to a specific organisation	8
The organisation's values regarding staff security and risk management ..	8
Striking a balance between the possible risks for the staff and the desired benefit for the population	8
The preferable security strategy	8
The local staff and the staff of partner organisations.....	9
3.3 Security planning at local level.....	10
Risk analysis.....	10
What a security plan should contain	11
What the organisations expect of their staff's behaviour	15
Co-operation with other actors.....	16
3.4 The organisation's obligations towards its employees.....	18
4. Further training in security awareness and management	20
5. Summary	21
The most important recommendations at a glance	21
Annex	22
Annex 1: Reference documents	22
A) Documents and material used	22
B) Documents and material used provided by aid organisations	22
Annex 2: Internet sources.....	23
Annex 3: Organisations and institutions that have been consulted	23

Foreword

The raising of awareness regarding staff security has gained considerable momentum over the last few years. In the Anglo-Saxon region, a rather lively debate is underway¹, and increasing attention is being given to the topic in Germany as well. While the importance of this issue is undisputed in German humanitarian organisations, it is addressed in very different ways in practice. In some organisations, the standards are already very high, i.e. documents have been compiled as well as curricula for further training, and corresponding resources to support staff have been established. In other institutions however, these elements of security management are not in place yet. Some organisations have formulated manuals and guidelines for action, while others merely refer to documents that are available, e. g. the guidelines of the International Committee of the Red Cross. In the interest of quality assurance in humanitarian aid and a harmonisation of approaches, reducing this discrepancy by setting minimum standards is an appropriate measure.

This document shows what minimum standards should look like and gives recommendations on how they ought to be set. It was initiated by VENRO and has been prepared with the financial support of the German Foreign Office. The project was presented and

discussed in the framework of the Co-ordinating Committee on Humanitarian Aid. The foundations for the statements in terms of contents are a survey among member organisations with reference to their documents, guidelines, curricula, etc. as well as an evaluation of existing literature on the topic (best practices). Around ten aid organisations were involved and provided their material (see list in Annex 3). In a workshop organised by VENRO in Bonn in November 2002, this document was discussed with the organisations involved, and it was subsequently revised.

The recommendations refer to the field of security, i.e. to issues regarding protection against violent attacks. The field of safety, i.e. issues relating to protection from accidents, disease, etc., is excluded. Although stress management is an important aspect of staff deployment abroad, it would exceed the volume of this publication.

The document expresses recommendations but does not intend to have them understood as imperative or as a blue print. Given the plurality of German humanitarian organisations it goes without saying that it is impossible to include all suggestions from all organisations to an equal degree.

Jürgen Lieser
Member of the VENRO Board /
Humanitarian Aid Department

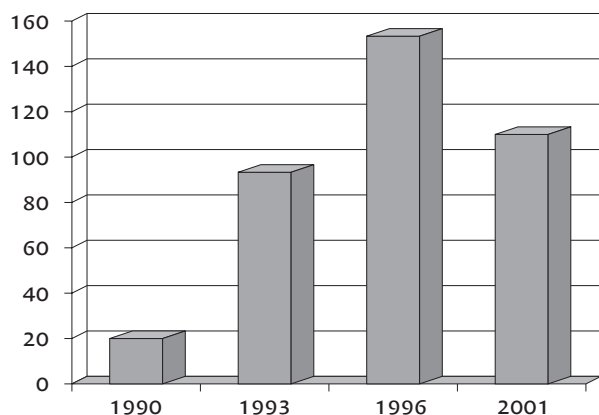
¹ E.g. in the Humanitarian Policy Group of the Overseas Development Institute in London, in the periodical »Forced Migration Review«, in the ICRC and UNHCR journals and on special Internet pages of the Relieweb.

1. Introduction

Since the beginning of the nineties, humanitarian aid and development organisations have been confronted with armed conflicts to an ever-increasing degree. In past years, the International Committee of the Red Cross (ICRC) was the only organisation maintaining a presence with expatriate staff to carry on with humanitarian activities during an acute armed conflict. This was possible because the Red Cross emblem was known throughout the world and, thanks to its unique status in international law, the ICRC was accepted and respected by the conflict parties as a neutral body. Today, a multitude of actors are present in large-scale crises and disasters. In addition to the wide variety of governmental organisations, hundreds of non-governmental organisations are often working at local level as well.

The worsening of the security situation for aid staff is reflected in the statistics of reported incidents.² The ICRC has reported a significant increase in the number of so-called »security incidents« per year.³

The United Nations refers to similar developments. From January 1992 to August 1998, 153 staff working for the UN lost their lives, and 43 were abducted. By May 2002, this figure had grown to 214 dead and 258 abducted persons.⁴ In 1992, the UN statistics referred to one fatality a month among their staff, one fatality every two weeks in 1993 and more than one a week in 1994.⁵ In spite of a number of improvements in the meantime, violence prevails, and



there are indications that the fatalities among the staff of non-governmental organisations have risen in particular.⁶ According to the ICRC targeting of its staff currently represents the greatest threat the organisation faces.

What are the reasons for these developments? Various aspects have to be mentioned here that relate on the one hand to the environment of humanitarian aid and on the other to humanitarian aid itself or the aid organisations involved:

- The number of violent, almost always inner-state, conflicts has constantly been growing, and therefore, so has the number of aid missions. The UN has recorded a dramatic increase in the number of its peace missions, which are almost always accompanied by humanitarian aid. In parallel to the UN activities, a large number of humanitarian organisations always commence activities to support the population in crisis-shaken countries as well. This coincides with an increase in the number of aid workers in action.
- A second reason is that non-compliance of the civil war parties with international humanitarian law is on the increase. They do not observe the internationally agreed rules on the protection of the civilian population in wars. On the contrary, the civilian population become a target of attacks and destabilisation policies. Whereas 90 per cent of the fatalities in the First World War were still soldiers, today, 90 percent are civilians. Some observers even claim that a soldier has a better chance of survival in many wars nowadays.⁷

2 While the statistics regarding these incidents are not standardised and no generally valid figures therefore exist, similar trends can be observed in the statistics of individual organisations.

3 Personal statement by the head of the ICRC security department.

4 United Nations 2002, p. 2.

5 Greenaway / Harris 1998, p. 4.

6 Sheik et al. 2000, p. 167.

7 Slim 1996, p. 5.

- A growing culture of impunity is coinciding with non-compliance with international law. Aid organisations are seen as simple targets that can be attacked without this having major consequences for those responsible. The UN reports that people responsible for staff being killed on missions have been held to account in just 7 per cent of these cases.⁸
- In parallel to the attacks on the civilian population, aid organisations are also being attacked. As supporters of the victims of wars and disasters, they are no longer regarded as neutral parties to the conflict. Moreover, since they transfer resources that are important for the warring parties, their aid to the suffering population gains a strategic role in warring.
- At the beginning of the 21st century, new problems are arising for aid organisations in several countries. On the one hand, there are more and more so-called »failed states«, i.e. states in which a generally accepted central government with a monopoly of power no longer exists. There, the above-mentioned developments have a particularly grave impact. On the other hand, international terrorism and attempts to fight it bear risks that also affect the options for the deployment of aid organisations.

But in addition to the environment aid measures are being carried out in, aid itself is changing. The international discussion focuses on two aspects⁹:

- Politicisation of humanitarian aid and its being used as a substitute for unsuccessful political action or as a means of covering up or justifying military incursions in crisis areas. It is observed that what used to be a clear demarcation line be-

tween humanitarian and military missions is now becoming blurred, which in turn is making it more difficult for aid organisations to maintain their neutrality.

- Nowadays, there is stiff competition among the aid organisations for financial support for humanitarian missions and the attention of the media that these missions attract. This can result in security interests being subordinated to the marketing strategies of organisations, with humanitarian aid also being provided in countries or situations in which the wellbeing and lives of staff are put at considerable risk.

If one examines the fatalities in humanitarian missions between 1985 and 1998, one arrives at the following results. Contrary to widespread opinion, accidents and diseases no longer constitute the chief reasons for these fatalities. In 68 per cent of the cases examined, intentional violence against members of aid organisations was the cause of deaths. This tallies with the figures of the ICRC, which reports of 77 per cent of fatalities resulting from violence. In contrast, car accidents accounted for just 17 per cent of fatalities, and non-intentional violence for 7 per cent. More accurate analyses of targeted murders of aid workers show that in 47 per cent of incidents, they were victims of raids on cars or convoys. While the statistics point in the same direction in assigning the murders to the origin of the victims, the overall picture tends to be less coherent. The various surveys report that between 58 per cent and 74 per cent of the victims were local staff.¹⁰

It has already been mentioned that these statistics do bear weaknesses. They nevertheless demonstrate very clearly that the threat to staff of aid organisations is a problem that humanitarian organisations really need to address.

⁸ United Nations 2002, p. 2.

⁹ See *Politics and Humanitarian Aid: Debates, Dilemmas and Dissension*, in: *Disasters 2001*. and Eberwein/Runge 2002.

¹⁰ For all figures see Brabant 2000, Annex 1, Sheik et al. 2000 and King 2002, which refers to the data bank »The Chronology of Humanitarian Aid Workers killed: 1997–2001« of the Reliefweb.

2. Overview of the level of debate on the topic

2.1 The position of the UN and international aid organisations

The UN and non-governmental aid organisations have already responded to this new threat. Some UN organisations are providing their entire staff with further training in the field of security (e.g. World Food Programme, WFP), while others are offering optional training measures. In December 1999, the UN General Assembly called on the UN Secretary-General for the first time to revise the existing security concept and make proposals for improvements. The subsequent report¹¹ recommends a significant upgrading of this topic and demands that appropriate financing be provided. So far, only a handful of countries have participated in financing security measures, while some others have announced that they will make financial contributions to this end. In this report, just like in the follow-up ones, the UN Secretary-General points out again and again that efforts made to ensure staff security represent neither a luxury nor a personal advantage, but that they are simply the price that the global community has to pay nowadays for the implementation of the UN mandate.

A similar state of affairs holds for the non-governmental aid organisations. If they wish to continue to provide aid in the context of violent conflicts, they have to improve security management within their organisation, upgrade their staff and make adequate arrangements for activities at local level. Different institutions approach this task in very different ways. In the case of American organisations and those whose documents come from an American sister organisation, it is conspicuous that, in particular, the guidelines for staff are strongly shaped by American jurisdiction regarding liability (see e.g. the World Vision International and Care International guide-

lines). Although the emphasis is on giving instructions for action among other organisations (what ought to or ought not to be done in certain crisis situations), a holistic approach to the issue of security is generally adopted whenever appropriate (e.g. in the guidelines of German Agro Action and in ICRC policy).

This approach goes beyond mere issues of the technical equipment required and the most adequate mode of response in hazardous situations, and it is based on the assumption of a mutual relationship between security and security measures on the one hand and good programme planning and implementation on the other. The most comprehensive account of this topic is given by Koenraad van Brabant in the »Good Practice Review« series issued by the Overseas Development Institute.¹² In the field of training material, the British non-governmental organisation RedR has distinguished itself with its »Security Training Guide«, which is freely accessible.¹³ Further basic documents on the topic are referred to in the list of further reading in the Annex.

2.2 The status of debate in Germany

In nearly all German organisations, awareness now seems to be firmly established that security or threats to it constitute an important topic for aid organisations. In the framework of the VENRO Working Group on Humanitarian Aid, the issue was debated in several sessions and adopted in several VENRO publications.¹⁴ In various German aid organisations, there are sets of guidelines that have either been compiled by the organisations themselves or by their international networks. Here, particular mention must be made of the guidelines of World Vision International (WVI), Care International, German Agro Action, German Red Cross/ICRC, Médecins Sans Frontières (MSF) and Caritas International/Catholic Relief Services (CRS).

However, few organisations have already developed a proper »security culture« and integrated the issue into all aspects of planning and implementation of aid measures. Also, there are considerable gaps in

¹¹ United Nations 2000.

¹² Brabant 2000.

¹³ Registered Engineers in Disaster Relief, seated in London. The Training Guide can be looked at at www.redr.org

¹⁴ VENRO 2002. (annually revised); VENRO 2000.

terms of reporting security incidents. Here, hardly any of the organisations have a sophisticated, structured system. Some organisations, such as the Malteser Foreign Department, Caritas International and German Agro Action, are currently in the process of working security aspects into project and human resource management.

Another field that has hardly been developed in Germany is security training. The annually updated VENRO publication¹⁵ provides an overview of training courses in humanitarian aid and also contains infor-

mation on courses in the field of staff security. However, the programmes run in Germany cannot be compared with what is run by the organisation RedR in the Anglo-Saxon region and by Bioforce in the Francophone region¹⁶. Nevertheless, German aid organisations have signalled a considerable demand for appropriate further training programmes. They would like to have a range of training courses with sufficient flexibility in terms of time both with regard to the frequency of the programmes and the length of the training courses.

¹⁵ VENRO 2002.

¹⁶ Seated near Lyon.

3. Improving security management in an organisation

Improving security management within an organisation involves a number of aspects. It is important that the topic is mainstreamed throughout the organisation. A coherent security policy has to be in place as well as detailed regulations on implementation at the level of local operations and straightforward statements of the organisation on what it expects of its staff. The organisation's obligations towards its staff should be clearly set out in writing, too. Last but not least, a management approach of this kind also addresses the issue of financing security measures.

3.1 Mainstreaming the topic within an organisation

There are different reasons for the discrepancy in organisations between being aware that the issue of security is important and insufficiently integrating this aspect into their activities. The arguments most frequently referred to are a lack of time and money and a general attitude of resignation that one has to reckon with such threats in project work and that not much can be done about it. Often, an increase in security management is also confused with less freedom of action at local level. In contrast, a holistic view of the subject stresses that it is precisely appropriate security management that enables operations to be carried out in dangerous areas in the first place.

In order to be able to establish these issues in an organisation, the following management instruments ought to be in place at the head office, tailored to the existing scope an organisation has and to its size:

- a forum that corresponding steps can be discussed and planned in
- a review of the procedures and regulations within the organisation from the angle of staff security (project planning, staff recruitment and secondment, finance administration, reporting and information processing)
- active involvement of and support by the organisation's management staff

- straightforward division of labour, definition of responsibilities and decision-making powers, schedules
- provision of human resources, labour time and operational means to support the mainstreaming process.

Whenever possible, the following steps ought to be taken or conditions be created at local level:

- conducting a risk analysis for the field of deployment
- drawing up a security plan
- regulating the distribution of activities, responsibilities and decision-making powers
- guidelines for incident reporting and analysis
- further training programmes
- enough financial means to remedy identified weaknesses.

It will be easier to accomplish the necessary organisational changes if the organisation's executive staff are clearly dedicated to coping with this task. The staff dealing with security management ought to have enough time and scope for activities concerning this task. Also, experience has shown that necessary changes are accelerated by incidents the staff of one's own organisation have been involved in or by pressure from outside, e.g. by potential donors. For example, the »EU Humanitarian Aid Office« (ECHO) enquires about the security plan of all organisations filing project proposals. And in the case of Afghanistan, the British government is even going as far as to have the security management of the recipients of funds checked locally by the embassy's security officer.

The United Nations has already introduced its system of minimum operating security standards (MOSS) covering the fields of security planning, training, telecommunications and equipment. All locations of assignment are obliged to fulfil these minimum standards by the 1st January 2003 or to at least submit an implementation plan showing by when the standards are going to be fulfilled.

3.2 Working out a »security policy« tailored to a specific organisation

Every organisation ought to define a general security policy for itself in which fundamental values and principles are represented. One statement here could be e.g. that the lives of the staff always take precedence over the protection of material values. This policy serves the purpose of arriving at a common understanding of the topic, defining a uniform practice of action and actively involving the staff in implementing the objectives. Examples of this are the chapter on »Werte und Prinzipien« (values and principles) in the guidelines of German Agro Action or the section on »Mandate« (mandates) in the MSF guidelines.

Since the size, mandate, working context, activities, etc. of the various aid organisations differ considerably, no generalised recommendation can be given here on the contents a policy of this kind should have. However, it is advisable to cover the following topics:

The organisation's values regarding staff security and risk management

What is our mission and vision for activities in the context of violent conflicts? What is our mandate and remit, and from what do we deduce the legitimacy of our assignment? What has priority in all circumstances and in every situation? What is our position on political and ethical or moral challenges that working in such a context entails?

Striking a balance between the possible risks for the staff and the desired benefit for the population

The decision whether an assignment is justified and legitimate has to be taken anew in each individual situation. Here the issue that is always at stake is how a balance can be achieved between the possible risk for the staff and the desired benefit for the target group. In this context, the following questions can be helpful, and should be discussed in a participatory process whenever possible:

- the risks the concrete assignment entails and the organisation's general readiness to take risks

- the need of the population and the organisation's mandate and portfolio
- the benefit and the positive impact of an assignment and the existence of a »humanitarian space«¹⁷
- options to reduce vulnerability to existing risks and improve security management in general.

Aid organisations are in a position to reduce their vulnerability by pursuing an appropriate security strategy.

The preferable security strategy

The security of aid organisations must not be conceived and treated in purely military terms, which are frequently mainly oriented on equipment, tactics and rules of behaviour. Since the work of aid organisations differs considerably from that of the military, its problems and options for action in the field of security are more complex. Generally, it can dispose of three strategies for action. The first one aims at deterrence, the second at protection and the third at acceptance and recognition.

A deterrence strategy aims at raising the risk of an attacker by threatening with counterviolence and inhibiting potential enemies. This includes political or economic sanctions as well as the exercising of diplomatic pressure. Armed escorts for aid shipments are also an element of this category. While this deterrence strategy is not particularly suitable for aid organisations, it does appear to be indispensable in some cases. However, the issue of armed protection for houses, convoys, etc. in particular requires that the head office clearly orients the staff at local level.¹⁸ Even if the decision usually has to be taken locally in a concrete situation, clear statements ought to be made for the benefit of this strategy for one's own activities and regulations ought to be in place on how a choice be-

¹⁷ This term is frequently used without any exact definition being given. It is based on the assumption that there has to be a minimum consensus between the conflict parties that humanitarian aid is important and ought to be provided. This consensus should also include the security of the staff working for the humanitarian organisations.

¹⁸ OCHA has issued recommendations referring to this in the framework of the UN Inter-Agency Security Management Network in collaboration with the Inter-Agency Standing Committee: Inter-Agency Security Management Network 2002.

tween conflicting objectives should be made and how the decision should be documented.

The second strategy is aimed at one's own protection and serves the purpose of making a potential attack more difficult. The possible protective measures fall into three categories. First of all there is protective equipment, second organisational rules and provisions and third co-ordination with other actors. Examples are burglar bars, bullet-proof vests, controlled access to offices and housing and other measures making attacks more difficult. Aid organisations almost always use this strategy too, especially as a protection against attacks by criminals. While such a response is understandable, it can result in a reactive »bunker mentality«. Dug in behind walls and barbed wire, one perceives the surroundings as a threat and loses contact with the people to the wellbeing of whom one really wishes to contribute.

This is why aid organisations primarily opt for the approach to gain protection by acceptance and recognition among the civilian population in project activities and in working with the target groups. This strategy is also referred to as an anthropological approach to security issues, or it is termed as software-oriented, as opposed to focusing on equipment and technology (hardware). Involving the people and the local authorities in the planning and implementation of measures is to help achieve their feeling responsible for the protection of the aid workers. Fear among the population of the aid organisations being withdrawn and a loss of international support is an important protective element. The effectiveness of this strategy was demonstrated, for example, in the case of the abduction of staff belonging to a German aid organisation in Tadjikistan. However, it is sometimes restricted by the civilian population being inhibited by the warring factions by threats of violence who then have to decide whether they want to be the victims of punitive campaigns or lose aid from outside. Moreover, the warring parties always have a perception of an aid organisation differing from that of the people benefiting from it.

Nevertheless, the civilian population remains an aid organisation's most important ally. However, recognition of the organisation's activities on the part of the population cannot simply be presumed but has to be earned. It is recommendable to again and again explicitly check the local »rate of acceptance« when a project commences and at regular intervals during its implementation. Here, local staff can contribute valuable services as a mediating and communicating body.

Often, there is a considerable discrepancy between how an organisation sees itself and how it is perceived by the local population in terms of how well it is known, its mandate, its work and, in particular, to what degree it is accepted.

Transparency in the criteria for the allocation of aid, continuous communication, how the staff behave and correct project planning are important elements. This is why all approaches towards »conflict-sensitive« project planning¹⁹ are immediately relevant to security. An existing source of tension in society may be heated up by the way that aid is distributed or by implicit ethical messages, e.g. by giving preference to an ethnic group in recruiting local staff. Thanks to failed project planning, they will be perceived as biased, or their operations may interfere with the activities of the warring parties. Thus they get into the field of fire and become targets of attacks. This also applies to activities that are explicitly aimed at resolving conflicts peacefully and may therefore be detrimental to the interests of »war-profiteers«. But if aid is planned and implemented with a view to reducing the existing sources of tension and promoting local capacities for peace, the framework conditions for the project activities will also frequently improve. And then the staff of aid organisations can be part of the solution rather than part of the conflict.

Since there are always different actors and different forms of threats in conflict-affected countries, a flexible mixture of the various strategy elements has to be found. Regular checks have to be made on whether the measures taken really correspond to the existing needs or whether they have to be adapted. Security problems will always arise if the chosen strategy does not correspond to the existing risks (anymore).

The local staff and the staff of partner organisations

An aid organisation's security policy should not be geared exclusively to the requirements and security problems of expatriate staff but should also consider the local staff.

An organisation's own local staff or that of partner organisations has a different vulnerability to security

¹⁹ E.g. the approach that has become well-known under the headword »Do no harm« emphasises that aid needs to be designed and implemented in a way that it does not aggravate existing conflicts. Other PCIA methods (peace and conflict impact assessment) have the same objective.

problems owing to its status in society. Since they are part of the social environment these people enjoy a certain level of protection, although working for an aid organisation means that they are also threatened. While protective measures have already been taken for expatriate staff in several aid organisations, local staff are often excluded from such measures. This state of affairs becomes particularly apparent in an evacuation, although it is not restricted to such an event. And given the general trend towards less foreign and more national staff, this gap is increasingly gaining significance and should therefore be bridged.

In their security policy, organisations should make clear statements on how far their obligation or readiness to provide for the welfare of their employees goes, what provisions are made, and where the limits of such provisions are. One of the issues at stake here is whether local staff can also be evacuated, whether wages continue to be paid for a certain period when international staff have been withdrawn, what is paid in the event of an accident and other aspects. Clearly communicated and transparently implemented regulations prevent nasty surprises when an emergency occurs. Often enough, security problems only emerge through local staff having different expectations regarding the organisation's conduct or making demands that the latter is not prepared to fulfil.

3.3 Security planning at local level

An organisation's security policy, which has been worked out at its headquarters, is put into concrete terms and regulations at local level. Staff require clear orientations as to how they are to respond to crisis situations and who can or has to make what decisions. Reporting on and analysis of incidents are also important issues that require guidelines. In addition to instructions for action, the imparting of methods with which the security situation can be assessed and adequate responses to it can be initiated is also recommended. In order to avoid disagreement and misunderstandings, it is helpful if the headquarters makes binding statements in a document for its staff on what its expectations of behaviour are in the country of assignment and what sanctions will be taken if these rules are not complied with. Explicit statements on this are, for example, contained in the guidelines of MSF, IFRC, GOAL, Handicap International Belgium and Care International. The contracts of employment

of various organisations, including the Arbeiter-Samariter-Bund, oblige their employees to be neutral, to observe local law, customs and religion in given countries and explicitly forbid them to bear weapons.

Security planning at local level includes a risk analysis, working out or drafting a security plan (which also makes provisions for reporting on incidents), a code of conduct for the staff in everyday project activities and guidelines for co-operation with other actors.

Risk analysis

Before a security plan is compiled at local level, a risk analysis ought to be conducted in a similar way to the assessment of the needs a target group of a planned project has. Here, potential threats are analysed on the one hand, and on the other, the vulnerability of the individuals working in the project is assessed. A risk analysis of this kind follows the equation $\text{risk} = \text{threat} \times \text{vulnerability}$. Although the threat itself can only be influenced minimally in most cases, aid organisations can reduce their vulnerability by opting for an appropriate security strategy. Local or international staff are vulnerable to certain threats to a varying extent. Age plays a role, as do nationality and, in several countries, ethnicity as well as, for example, one's status within an organisation or the profile of the organisation itself.

Particular attention ought to be given to differences in vulnerability between men and women. Sexually motivated assaults almost exclusively affect women, which is why special precautions ought to be taken to protect female staff in countries in which such threats are very likely to occur. On the other hand, the situation should not be used as an excuse not to employ any women right from the start. In some countries and situations, men are in more jeopardy than women, especially if the attackers' main aim is to demonstrate their power and strength. And if media coverage is of special importance, for example in the case of an abduction, woman hostages and children are frequently released at an early stage to gain a better public image.

The following questions are asked in analysing threats: Who represents a threat? Why? What are the possible targets for attacks? How and where could attacks be launched? Checklists can be drawn up for these considerations, and security levels can be de-

fined to classify certain situations. The UN has a five-phase model, while various aid organisations work with four-phase models (e.g. MSF, WVI, Care International, Caritas International Afghanistan). Phasing offers the advantage of a certain degree of standardisation of responses and a guarantee that certain provisional measures are taken without having to spend much time on planning and co-ordinating in an acute situation. Moreover, the events or threat scenarios resulting in a certain phase are defined right from the onset. This prevents staff from gradually getting used to a deterioration of their situation and only becoming aware of this when it would have been better to leave the region or the country when it is already too late. The disadvantage of phasing is that the system is rather rigid. Often, the local situation changes very quickly, and there is not enough time to determine the transition from phase x to phase y. Furthermore, there is a danger that staff may have a false sense of security if the country of assignment has been graded as relatively unproblematic. In these countries too, security problems can arise almost overnight, or individual persons or organisations can become a target for certain reasons, even if the general situation appears to be relatively stable.

So an ongoing monitoring of the surroundings with regard to security issues is always recommendable. As an alternative to the security levels, risk analysis can be adopted as an integral element of day-to-day project management. Gathering information from different sources and continuous dialogue with as many people involved as possible are important ways of always ensuring an optimum up-to-date assessment of the situation. Information can be processed with the aid of a matrix on the horizontal axis of which the probability of the occurrence of a threat is entered while the vertical axis shows the impact. This matrix can be used to determine how serious a risk is. Consideration should subsequently be given to how the risk can be reduced. Is it possible to lower the probability of its occurrence? Is it possible to reduce the impact on individual project staff or the programme as a whole? Can the predictability of the risk be improved? Are there opportunities for the organisation or the staff to reduce the level of exposure to the risk?

On the basis of such a risk analysis, the security strategy is chosen that is most suited to the concrete situation in the project area. As already explained, it should be a mix of the different approaches. Depending on the organisation and the country of assign-

ment, this strategy will assume different forms, but it will be formulated in concrete terms in the security plan for the respective country and translated into instructions for action to be taken for the staff. One example to be mentioned here is the security plan of Caritas International Afghanistan, which specifies the general provisions made in the CRS guidelines.

What a security plan should contain

The central element of an organisation's »security architecture« is the definition of responsibilities and (decision-making) powers. On the one hand, they ought to be included in the job descriptions for the staff, and on the other, the security plan should contain clear statements on the employees' authority to give directions and the duty to comply with instructions.

The process of compiling a security plan²⁰ is just as important as the plan itself. General Eisenhower is quoted in this context as having said: »A plan is nothing. Planning is everything.« But a security plan will only improve an organisation's security management if it meets certain quality standards and is integrated into all aspects of project management. If an organisation expects its employees – whether it be local or expatriate staff – to comply with the plan, they have to be involved in compiling and updating it. The local staff in particular has information and insights that are of considerable value in correctly assessing the situation. Once an initial draft has been completed, the plan should be tested, and it always ought to be updated when the threatening situation or the vulnerability of the organisation or the staff has changed.

Most commonly, instructions for action in various situations or threatening scenarios form a key element of security plans. Depending on an organisation's culture of security or the legal situation in its home country, this will frequently result in these plans degenerating into bulky compendia containing long lists of what to do or not to do in any conceivable event. There are serious doubts as to whether the staff a) read these thick books, b) can memorise the countless recommendations and c) such »shopping lists«

²⁰ InterAction provides its member organisations with an excellent, concise summary of the most important aspects in compiling a security plan. They can be looked at at www.interaction.org.

do not tend to result in weariness and an attitude that »it is all so complicated that I prefer to rely on my own common sense«. Objections of this kind are justified, so it ought to be assessed locally what concrete threatening scenarios instructions are given for. Attention should be given to a user-friendly format and layout. Good examples of this are the ICRC's handy set of

guidelines called »Staying Alive« or the WVI manual.

This is what a model for a security plan could look like: At the beginning, statements are recommendable on the objective of the plan, the compilation process, implementation and updating as well as on the circle of people who are to observe it. A second chapter could provide background information on the organisation (mandate, principles, security policy), on the local situation (political, economic, historical, military, etc.) and on the results of the risk analysis. The aim of such a chapter is to provide newcomers and visitors with an overview of the situation as it is so that they can gain a better understanding of the subsequent instructions for action.

Many security plans offer extensive instructions on how to act in concrete situations, which are referred to as »standard operating procedures« (SOP). These instructions refer to recurrent events or pre-defined hazard situations. They should always answer the following questions: What should be done or not done? How is a procedure carried out? Who implements it and together with whom? When and where is it implemented (frequency and sequence)?

This is why most security plans contain SOP's on the following topics observing the following questions:

► **Organisational measures**

What information has to be available? At which locations? Who has access, and how is it secured? How is it kept up-to-date? What maps or other documents are required? Which forms have to be used?

Typical table of contents of a security plan:

Introduction

- Date and author
- Objective
- Elaboration process
- Intended users

Background information

- Mission statement
- Context analysis
- Mandate of the organisation
- Risk analysis
- Security strategy

Standard Operating Procedures

- Transport of personnel and material
- Site security
- Communications
- Handling money
- Incident reporting
- Landmines (if applicable)

Contingency Plans

- Evacuation
- Medical evacuation
- Kidnapping
- Death of staff
- Natural disasters (if applicable)

Supporting Documents

- List of staff, addresses, telephone numbers, passport details, blood group, family contact details
- List of international organisations, contact persons, contact details including radio frequencies
- Resource people (medical personnel, UN Security Officer, immigration and travel agencies)
- Maps indicating assembly points, evacuation routes and preferred route

The following is of special importance:

- **Information regarding passports and visas** (Passport numbers, visa numbers, expiry dates)
- **Information regarding contact persons** (Names and telephone numbers)
- **Medical information** (blood group, special medication)
- **Contact details of doctors, ambulance etc.** (Name and telephone numbers)

► Transporting staff and materials

How are travels outside the location of assignment to be dealt with? What measures are to be taken regarding the roadworthiness of vehicles? What maintenance work is to be carried out before a trip commences? What equipment for emergencies should always be included in the luggage? How is travelling in convoys organised and carried out? How is the transport of materials controlled? What should be observed in the event of an accident? How should one respond to traffic checks or roadblocks?

The following is of special importance:

- **Vehicle choice**
(4-wheel drive: yes or no, label and model, new or second-hand cars, own fleet or rental cars)
- **Vehicle safety**
(Equipment, maintenance, training the personnel in repairs)
- **Style of driving and behaviour**
(Speed limits, seat belts, recruitment and training of drivers, policy regarding driving at night, behaviour if causing an accident)
- **Approaches to passengers**
(Policy regarding lifts for armed personnel and the police)
- **Journey planning**
(Team briefing and debriefing, collection of information, maintaining contact with the base station)
- **Checkpoints**
(Preparations before reaching the checkpoint, behaviour at the checkpoint, policy regarding handling over documents)
- **Convoys**
(Planning, constituting and leading a convoy, behaviour and discipline)

For more extensive information see Brabant 2000, Chapter 8.

► Communication

Who communicates when, how, how often and with whom? What means of communication are there? How are they used? How are staff trained to use them? What rules are to be observed regarding the form and contents of communication? Which rules apply in an emergency?

The following is of special importance:

- **Choosing telecommunications**
(HF-radio, VHF-radio, mobile telephones, satellite telephones and email)
- **Setting up the equipment**
(Operational requirements, vulnerability for failure and sabotage, prices, maintenance, network compatibility, administrative permissions and licensing)
- **Operating the equipment**
(Installation of the base station and mobile units, power supply, safety)
- **Training the users**
(Technical details, rules and regulations for calls, discipline, distress and security calls)
- **Regulations on communication**
(Tasks and competence, frequency, regulation in case of an incident, operating hours)

For more extensive information see Brabant 2000, Chapter 17.

► Protection of premises

Where and how are offices and residences or warehouses selected? How are they protected? Who are they guarded by? Where are the emergency exits, and what are the vulnerable points? Who keeps which keys? What means of communication are there? Who has access, and how is it controlled?

The following is of special importance:

- **Site selection**
(Neighbourhood, proximity to strategic infrastructure, compound, landlord)
- **Physical criteria**
(Site, access and ways out, parking, illumination, burglar bars, power supply)
- **Managing access**
(Visitors, keys)
- **Guarding**
(Own guards or security firms, police patrolling, equipment of the guards, management of shifts and duty)

For more extensive information see Brabant 2000, Chapter 9.

▶ Handling money

How is cash transported and kept? Who has access to the cashbox and the safe? Who has been informed about forthcoming money transfers? How can modes of payment be arranged so as to minimise security risks?

The following is of special importance:

- **Using different ways of payments**
(Reducing the use of cash, spreading the risk)
- **Frequency and responsibility**
(Reduce the numbers of transfers, just-in-time payments, transferring the risk to banks and contractors)
- **Discretion and predictability**
(Choice of personnel, limiting knowledge, avoid payment routine)

For more extensive information see Brabant 2000, Chapter 11.

▶ Reporting

When should a report be written? Who reports how and to whom? What is reported? Who has access to this information? What format should the reports have?

The following is of special importance:

- **Type and frequency of reporting**
(Regular reports and incident reports, format, content)
- **Responsibility**
(Responsibility for reporting and analysis both locally and in head office, information sharing)
- **Incident analysis**
(Motive, reason for choosing the victim, consequences and follow-up)
- **Information management**
(Confidentiality, perceived »intelligence gathering«)

For more extensive information see Brabant 2000, Chapter 16.

In parallel to organising staff reporting at local level on incidents, arrangements should also be made on who the reports are submitted to at the headquarters. How are they analysed, and who should initiate what subsequent steps if required? A careful analysis of the reports can give valuable clues on how to avoid a similar event in future.

In addition to the instructions regarding recurrent events or procedures it is also recommendable to make contingency plans for special cases, in particular for the event of an evacuation (for security reasons or owing to medical problems), for the event of an abduction, a fatality and also for other high and at the same time probable risks.

▶ Evacuating staff for security reasons

Generally, the problem always exists in the case of an evacuation or relocation of staff that such a situation can only be planned in advance to a limited degree. It is nevertheless advisable to make some general preliminary considerations in order to at least reduce the hassle and turmoil of an emergency and create awareness of various aspects among the staff.

In planning an evacuation, the decision-making powers have to be settled first of all. Who decides whether an evacuation should be carried out? If there are different opinions, is it the view of the headquarters that is decisive or the assessment made by the staff in the country? What is the procedure if staff wish to leave in advance or want to stay? If it is government organisations, the authority to give directions among the organisation and the German Embassy or the Federal Ministry for Economic Cooperation and Development (BMZ) and the Foreign Office should be referred to in the plan, and the consequences for the staff should be clarified. In particular, the role and tasks of the Crisis Response Centre (KRZ) of the German Foreign Office have to be observed (see »Co-operation with other actors«, pp. 16).

The decision in favour of or against an evacuation ought to strike a balance between the threats to the staff and the benefit of the activities for the population and other possibilities to minimise risks. Furthermore, the response of other organisations, possible recommendations by the German or other governments to leave the country, the impact of the expatriate staff's departure on the security of the local staff and the possibility of returning after an evacuation in

order to carry on the project activities should all be considered in the decision.

Various organisations have also developed a phase model for evacuations (e.g. Care, WVI, CRS), while others merely restrict themselves to clarifying the following aspects in advance: Who is evacuated when and where to? How are the staff contacted? What escape routes are there? Where are the meeting points, and what form of transport can be used? What personal data and documents are required? What provisions are to be made regarding personal security and safeguarding of material for the local staff? What should be done with equipment, warehouse stores and office buildings and residences?

Planning these aspects in advance helps to reduce possible confusion in an emergency and settles right from the start what the staff can expect of the organisation in the case of project activities being suspended. Provisions for the security of those who are not to be evacuated must also be considered. This is particularly important for the local staff in order to avoid misunderstandings and disappointment. The fact that it is almost always only the foreigners and, frequently, computers and, sometimes, cars that are evacuated while the local staff are abandoned to their fate is a highly sensitive problem. Even if there is probably no general solution to it and an ethical dilemma will always arise, transparency and consistency in treating these issues can contribute considerably to reducing the severity and volatility of the topic. What is also important is discussing these issues while they are still at a hypothetical level. Such difficult aspects can no longer be dealt with and communicated appropriately under strain and at the moment the emergency arises.

► **Evacuating for medical reasons**

Here too, the decision-making powers have to be settled clearly, while the aspect of bearing the costs also plays a role. It has to be clarified who informs whom about evacuation, where staff are evacuated to (to a neighbouring country or to Germany), which formalities have to be observed in the country (e.g. landing permits for the aeroplane), who accompanies the journey, what accompanying documents are required and who receives the evacuees in the target country and continues to look after them.

► **Abduction**

In the event of a staff member being abducted, a crisis management team ought to be appointed immediately that decides on the following issues: Which official bodies in the country of assignment and in Germany have to be informed? Who should not be informed (for the time being)? Who negotiates with whom at what level? Where is the information gathered, and how is it processed? How are the next of kin informed and cared for? How are press relations dealt with? What offers are there for a victim of an abduction after the abduction is over?

In such a serious case, the Foreign Office Crisis Response Centre (KRZ) is the most important body to contact in Germany, and as a rule, it assumes control of the entire crisis management process. So in making preparations, the aid organisations ought to concentrate on what internal organisation policy they wish to pursue with regard to the above-mentioned questions and how they wish to regulate decision-making powers.

► **Fatality**

Straightforward regulations referring to the following aspects ought to be in place for the event of a local staff member being killed while working for the organisation: informing the next of kin and the authorities, paying for funeral costs and compensation payments for the bereaved. Here, it is particularly important to observe local laws and customs to avoid causing the family additional hardship and, on the other hand, prevent possible misconduct from turning into a further security problem.

In the event of the death of an expatriate team member in the country of assignment, plans are required for notifying the next of kin, the transfer of the mortal remains, sending the belongings of the deceased person home and, possibly, dealing with insurance issues (necessary documents, schedules to be observed, etc.).

What the organisations expect of their staff's behaviour

Setting out from the insight that the security of aid organisations is not merely a question of equipment and technology but crucially depends on people's be-



Security training of the »Alliance 2015« in Kabul / Afghanistan, November 2002

haviour and the way that projects are implemented, in addition to regulations on action to be taken in the event of a concrete threat, expectations also have to be clarified that an organisation has of its staff in its day-to-day operations. These issues can be covered in a special chapter of the security plan or in a separate document that ought to be referred to in the labour contracts. Some organisations have developed forms with which employees commit themselves to observing certain regulations, as is the case with the Malteser Foreign Department and Caritas International, or they issue instructions, like the Deutsche Gesellschaft für Technische Zusammenarbeit (GTZ) or German Agro Action.

General issues of good project implementation (involving the population and the local authorities, transparency and consistency of activities, communicating with the beneficiaries and groups that do not benefit from the project, etc.) ought to be an integral part of project management and be imparted in training courses rather than by written documents.

The code of conduct staff members have committed themselves to comply with (e.g. referred to explicitly in the documents of Handicap International Belgium and GOAL) aims at promoting an understanding of the relation between the type of project implemen-

tation and the personal behaviour of the staff on the one hand and the threat scenarios on the other. Employees are thus supposed to understand that they have concrete options in everyday life and work to reduce their vulnerability to certain threats. Additional important aspects such a document should contain include teamwork, each individual's responsibility for his or her security and that of the colleagues and, in particular, sensitivity towards other cultures (issues regarding clothing, alcohol consumption, the status of religion, relations between men and women).

Statements on sanctions applied in the case of non-compliance with guidelines on behaviour should either be contained in such a document or directly in the labour contracts. The disciplinary or legal consequences employees have to reckon with depend on the organisation itself. The consequences that may result from breaching regulations once again show the employees their status in the organisation.

Co-operation with other actors

In many countries of assignment that aid organisations operate in, so many actors are often represented that neither the civilian population nor the military

can distinguish them from one another. This is why action or failure to act on the part of one organisation will almost always have repercussions on others. While close co-ordination is already taking place in various fields, it could certainly be intensified and is also of importance from a security angle. The UN addressed this with guidelines early in 2002 that are aimed at regulating collaboration between UN agencies and aid organisations.²¹

With the Office for the Coordination of Humanitarian Affairs (OCHA), the UN has created a coordinating body for issues related to contents, while UNSECOORD (Office of the United Nations Security Coordinator) deals with security issues.²² The head of the latter is appointed by the Secretary General and has the task of formulating the UN security policy for all UN agencies and programmes. In each country in which UN staff are active, the Security Coordinator appoints a Designated Official (DO) for the topic of security. Often, he or she is the Resident Humanitarian Coordinator. He or she appoints a security management team in which the responsible officials of the various UN agencies operating at local level deal with security issues. In many countries, UNSECOORD is represented by Field Advisors, sometimes also outside the capital. As a rule, the DO announces weekly security meetings of all humanitarian organisations that above all serve the purpose of sharing information. Frequently, the UN also offers its services to aid organisations, such as a radio station that is manned round the clock or daily information on whether certain trunk roads are passable. In the case of non-governmental organisations, co-operation is on a voluntary basis, but it is urgently advised. To facilitate co-operation, the UN recommends the designation of a focal point for security issues among the aid organisations.

An evacuation with the aid of UN aeroplanes will also be co-ordinated by UNSECOORD should the need arise. If possible, all foreigners registered at the UN as well as non-residential local staff are evacuated. Every organisation ought to take note of the fact that the most up-to-date information on the staff to be evacuated is available at the UN. However, only those organisations have a right to be evacuated that have signed a memorandum of understanding with the UN, which

In Afghanistan, a number of NGOs jointly recruited an NGO Security Advisor. He is the focal point for security matters for contacts with the UN and plays a coordinating role in the NGO community. He informs the organisations, participates in security meetings of the UN and the international military force and advises on the development of security plans.

in return contains the obligation to comply with all UN security regulations.

Sharing information on the situation in the country and on possible incidents is of considerable importance for an up-to-date and comprehensive risk analysis. However, it always has to be borne in mind that information is frequently second or third-hand, and that things are often distorted by informers depending on the way they see them. Moreover, an incident that may seem acceptable to one person can already represent a harbinger of disaster to another. Frequently, organisations avoid sharing information about incidents they have been involved in for fear of their being partly blamed for the event or its coming about being interpreted as a weakness on their part.

Organisations that are members of an international network frequently co-operate very closely with these partners in a country of assignment. This creates an improvement in the flow of information on a confidential basis and enables resources – both human resources and equipment – to be concentrated.

In any country in which security problems arise, the German Embassy takes precautions. It works out crisis plans in which the governmental organisations are integrated on a mandatory basis and the non-governmental organisations on a voluntary basis. Staff of government organisations are accordingly required to comply with the Embassy's instructions. In particular, they have to observe recommendations to leave a country.

The German Embassy's protective measures may be:

- a general warning to the people under its custody
- issuing protection certificates and protection badges for houses and road motor vehicles
- transmitting news or reports on the security status in the project region to the Foreign Office
- evacuating.

²¹ United Nations Security Coordinator February 2002.

²² For more details on this, see Brabant 2000, Annex 3.

Contact:

Tel.: +49-30-50 00-29 11

Fax: +49-30-50 00-44 98

E-Mail: Lagezentrum@auswaertiges-amt.de oder
Lagezentrum@diplo.de

The Foreign Office's Crisis Response Centre (KRZ) in Berlin can be called on round the clock and is the contact for emergencies abroad occurring outside service hours. Its tasks include the early recognition of crises, precautionary measures and crisis management. As soon as a critical situation abroad has been defined as a »crisis«, overall control of subsequent handling of the crisis is transferred to the KRZ. In crisis management, the KRZ provides its experience and personal and technical resources, and it also assumes a co-ordinating role vis-à-vis other operational units of the Foreign Office that are consulted in the context. In order to be able to perform this co-ordinating role, and in order to ensure that information and decision-making routes to the Foreign Office's executive level are as short as possible, the KRZ is located at the latter level. In a crisis event, a crisis committee is as a rule appointed on the secretary of state's instructions. It is the Federal Government's crisis committee at the Foreign Office. It takes all decisions on crisis response in a swift, unbureaucratic manner and assigns corresponding tasks to the individual actors to be dealt with immediately. This crisis committee has a core team of members comprising the KRZ, the minister's office, secretaries of state, the respective country department, and in addition, in the framework of a modular concept, other operational units of the Foreign Office and the Federal ministries and subordinate authorities that are required for crisis management, e.g. the Ministry for Economic Cooperation and Development, the Ministry of Defence, the Federal Chancellor's Office, the Ministry of the Interior, the Federal Intelligence Service and the Federal Office of Criminal Investigation. Regarding the staff of aid organisations, the crisis committee takes the necessary decisions in co-operation with the Ministry for Economic Cooperation and Development. The KRZ also seeks close contact with the decision-makers of immediately affected organisations in Germany. In the event of a crisis, these organisations should get in touch with the committee as early as possible. The embassies always play an important role in crisis management and

form an embassy crisis committee that is in close contact with the KRZ and co-ordinates crisis response measures at local level.

The Federal Ministry for Economic Cooperation and Development monitors the security status in the individual developing countries and projects on the basis of embassy reports, the representatives of governmental aid organisations and other suitable information sources. As soon as there are any signs of the security status deteriorating in a country of assignment, as in acute cases of tension and crisis, the Ministry's crisis committee initiates protective measures that are binding or, in individual cases, may be recommendations in the interest of the security of expatriate staff and their next of kin.

3.4 The organisation's obligations towards its employees

In assignments in countries with security problems, the employing organisation has a special obligation to provide welfare services for its employees. In the framework of the People in Aid network (The People in Aid Code of Best Practice), the signatory aid organisations commit themselves in principle 7 to pay particular attention to the issue: »We take all reasonable steps to ensure staff security and well-being. We recognize that the work of relief and development agencies often places great demands on staff in conditions of complexity and risk. We take all reasonable steps to ensure the security and well-being of staff and their families.«²³

Here, the establishment and continuous updating of important personal data is referred to in the administrative sector. Up-to-date data of every staff member such as address, telephone numbers, number, age and sex of next of kin living in the country, pass and visa numbers as well as dates of expiry and contact addresses of next of kin in Germany should be available at the headquarters and, if it exists, at the country office. In addition, necessary medical information should be provided (blood group, permanent medication, other important information). If possible, this should be kept separately and be protected from unauthorised access.

²³ For the code text, look at www.peopleinaid.org.uk/code/code13.htm

It is now undisputed among aid organisations that staff working in crisis situations are subject to special stress that may result in security aspects no longer being given adequate consideration or staff being so overworked that their behaviour becomes a security risk. This is why staff in crisis regions ought to be given a regular opportunity to leave their country of assignment for rest and recreation (R&R). The UN's R&R system entitles staff to a week's special leave every three months. Several aid organisations offer their employees similar options. Staff do not always take advantage of this offer since the impression frequently arises that it is impossible to interrupt activities. In such cases, it can be useful for the head office to keep an eye on whether these staff members are still fit for service or whether there are clear signs of a burn-out. In addition to this offer of breaks, some organisations provide supervision programmes, i.e. psychological counselling and care during and/or after assignment to a crisis region.

Insurance cover is of particular importance in crisis countries. The recommendations compiled by VENRO referring to this issue provide an important orientation.²⁴ It is advisable to check the policies that have been signed on a routine basis twice a year: Are the persons referred to the right ones? Are all current countries of assignment covered? Do exclusory clauses apply owing to new assignments? In addition to insurance cover for expatriate staff, it ought to be checked whether local staff can be insured as well. If this is not possible in Germany, policies on the international market or at local level can be considered. Particularly in the case of high-risk assignments, such as mine clearance, sufficient insurance cover ought to be a precondition for the commencement of activities, also to protect the organisation against possible high claims for damages, the rejection of which could in turn result in threats. The organisation should also

clearly communicate to its staff what equipment they can reckon with. If an organisation requires its staff to be available round the clock, it has to provide the equipment needed to this end. It is also important to demonstrate sensitivity in handling requests from the projects regarding new communications equipment since turning down procurements in this field for budgetary reasons can frequently result in frustration. Staff at local level can then get the feeling that concern about security is not taken seriously enough. Once again, the treatment of local staff is a difficult and sensitive aspect. For example, if expatriate staff are provided with cars with Codan radios but local staff do not even get handheld sets, the impression can easily arise that people's lives are valued differently. So here too, a transparent, consistent and well-communicated approach is crucial.

Financial bottlenecks should only play a role in decisions relating to security aspects in exceptional situations. Either a separate budget item should be contained in an organisation's overall budget (economic plan) or a certain percentage of every project budget should be earmarked for this purpose. Wherever it has not yet evolved, an appreciation of the need for such expenditures should be actively promoted among the donors. Funds of this kind can be used for training measures and/or equipment. In the case of project budgets, it ought to be made clear to the donors as well that this financial effort is the precondition for the implementation of the project. It is also advisable to adopt references in every application for funding to the degree to which the success of the measure would be jeopardised in the event of security problems and the organisation gives priority to staff security. The readiness to spend money on staff security is an indicator that is clearly visible to others of the effort an organisation is making in this field of its human resource management.

²⁴ VENRO 2000, also see Brabant 2000, Annex 6.

4. Further training in security awareness and management

»I am instructing the senior officials that security training and security awareness must be provided to every staff member. This is the single most effective means of minimizing risk.«

UN-Secretary General Kofi Annan

Training and further training for staff in security awareness and management is a central aspect of making concrete improvements to the local working conditions. Not only do the staff acquire know-how and methods, but they also develop a different awareness of the situation and are more self-confident in widening their scope of activity. If staff are committed in their job descriptions to take security measures, conduct analyses, compile security plans, etc., it is important in recruiting them to settle whether they dispose of the appropriate know-how. If not, they should be given the opportunity to acquire it.

Before they go abroad, all employees ought to be offered the opportunity to take part in security training themselves. Up-to-date information on training measures can be provided. Organisations running their own preparatory courses can adopt modules on staff security in their syllabus. In addition, these courses can also include concrete exercises on how to respond to an attack, etc. However, the exercises should be appropriately backed up psychologically, and participants should be given due attention. The advantage of training during the preparatory period is above all that it can be fitted into schedules more conveniently and that the participants are not yet subject to the immediate pressure and stress of an assignment. However, this can also be a disadvantage because the training contents will of course then be more abstract and cannot be tailored so specifically to the assignment situation the individual will be facing. Training courses run during an assignment and specially for the staff working in it can elucidate the concrete conflict and integrate the immediate experience of the participants to show how the security management approach can be established in the concrete project.

For reasons of confidentiality, some organisations prefer to only have their own staff admitted to a training course. The advantage of this is that very sensitive

information can also be passed on in a very intimate framework and delicate issues can also be addressed. The disadvantage is that staff members are left to stew in their own juice and that there is a lack of information and experience from other organisations. Here too, it is recommendable to work in the context of an NGO network or together with a small number of selected organisations with which an institutional confidential relationship has been established.

It is also important to involve local staff in the running of further training measures. For one thing, this is fair and complies with a caring approach. But it makes sense in terms of transparency and with a view to complementing perspectives and experience as well. For example, a comprehensive risk analysis can only be carried out in a workshop if various staff groups are represented that contribute their perspectives, resulting in the different threats and vulnerabilities of all employees being considered. Some particularly sensitive issues, such as money transfer, should not be discussed in a larger group, but for other topics, such as reporting an incident, it is of crucial importance that everyone is aware of the respective regulations.

So far, the range of further training measures has reflected the importance of the topic and the demand to be reckoned with neither in terms of its contents nor of its volume. In the European context, there are two organisations that have specialised in the field of security training for aid organisation staff: the organisation RedR in the English-speaking region, and Bioforce in the French-speaking region. However, the latter only run their courses in France. They are particularly suitable for the preparation of missions and focus more strongly on the personal security of the individual. For example, concrete behaviour training is carried out in role plays. There are different course modules that can also be offered separately for individual organisations. RedR runs its courses both in the United Kingdom and in developing countries, about two to three times a year in the UK and about four times in conflict countries. RedR has various modules as well, e.g. for employees who are on a concrete assignment, for executive staff, for the logistic

field and also training for trainers. As a rule, the courses last three to five days and cost about 400 US \$.

In Germany, there are hardly any further training measures that focus specifically on the topic. But various courses are run that do at least address certain aspects of staff security.²⁵ Elements are contained in Practice-Oriented Training Humanitarian Aid, at the Association for Development Cooperation (AGEH) and InWent and within individual organisations (German Agro Action, World Vision). And the German Red Cross offers all those who are interested (also non-staff members) a training course in addition to the further training offers of the ICRC or the Red Cross Federation. The newly founded Centre for Peace Assignments (Zentrum für Friedenseinsätze/ZIF), which

is seated in Berlin, prepares people for assignments in UN and OSCE missions and also addresses security aspects in its courses. From 2003 on, the Academy for Crisis Management, Emergency Planning and Civil Defence (AKNZ) also wants to run such courses.

For organisations wishing to run their own seminars, support is being offered by a number of donors. The EU Humanitarian Aid Office (ECHO) has already explicitly called for proposals for its grant facility for courses in field of staff security, and OFDA (Office for Disaster Assistance, part of USAID) has made a call for proposals, too. In the framework of the Co-ordinating Committee on Humanitarian Aid, the actual demand for further training should therefore be established and financing options should be explored.

5. Summary

The most important recommendations at a glance

At an organisation's headquarters, the following steps ought to be initiated:

- working out a general security policy at the headquarters;
- settling responsibilities and decision-making powers and including them in job descriptions and work routines;
- clarifying what behaviour the organisation expects of its employees;
- establishing what the expatriate and the local staff may expect of the organisation;
- providing information on or creating access to further training measures;
- providing financial means for training and equipment.

At local level, the following steps ought to be taken or the following respective conditions ought to be created:

- settling the allocation of tasks, responsibilities and decision-making powers;
- carrying out a risk analysis for the field of assignment;
- compiling a security plan;
- regulations on reporting and analysing incidents;
- regulations on collaborating with other actors at local level.

To finance security measures:

- lobbying activities so that costs in the field of security can be included in the aid agencies' project proposals;
- providing budgets for training and equipment, either in the general budget of the organisation or as a flat rate of project proposals or as a separate budget line.

²⁵ See the annual brochure issued by VENRO and titled »Qualifizierungsangebote in der Humanitären Hilfe« as well as the data bank HATI (Humanitarian Assistance Training Inventory) on training offers in the Reliefweb www.reliefweb.int/training

Annex

Annex 1: Reference documents

A) Documents and material used (important documents are in bold print)

Bettati, Mario, Protection for non-governmental organisations on hazardous duties. Report on the results of a UIA survey, 1999. (www.uia.org/surveys/batreng.htm)

Brabant, Koenraad van, Operational Security Management in Violent Environments – A Field Manual for Aid Agencies, Humanitarian Practice Network (HPN), Overseas Development Institute, London 2000.

Brabant, Koenraad van, Mainstreaming Safety and Security Management in Aid Agencies. Overseas Development Institute / Humanitarian Policy Group Briefing Number 2, March 2001. (www.odi.org.uk/hpg/papers/hpgbrief2.pdf)

Brabant, Koenraad van, Security Training: where are we now? In: Forced Migration Review 4, April 1999. (www.fmreview.org/FMRpdfs/FMR04/fmr402.pdf)

Eberwein, Wolf-Dieter und Runge, Peter (Eds.), Politik oder Hilfe? Neue Herausforderungen für ein altes Politikfeld, Münster 2002.

Greenaway, Sean / Harris, Andrew J., Humanitarian Security: Challenges and Responses. Paper presented to the Forging Peace Conference, Harvard University, March 1998. (www.reliefweb.int/library/documents/echoanser.html)

InterAction, The Security of National Staff: Toward Good Practices, July 2001. (www.interaction.org/files.cgi/531_sec_nationals_staff_final_doc.doc)

Inter-Agency Security Management Network, Use of Military or Armed Escorts for Humanitarian Convoys, Conference Room Paper 13 (prepared by OCHA), Vienna May 2002.

King, Dennis, Paying the Ultimate Price: Analysis of the deaths of humanitarian aid workers (1997–2001), OCHA, January 2002. (www.odihpn.org/report.asp?ReportID=2454)

Kreidler, Corinna, Die gefährdeten Helfer. Nothilfe braucht neue Sicherheitskonzepte, in: Entwicklung + Zusammenarbeit 11, November 2001. (www.dse.dezeitschr/ez1101-3.htm)

Martin, Randolph, NGO Field Security, in: Forced Migration Review 4, April 1999. (www.nrc.no/global_idp_survey/FMR/99-4/Martin.htm)

Politics and Humanitarian Aid: Debates, Dilemmas and Dissension, in: Disasters, 2001, Nr. 25, S. 269–372.

Sheik, Mani et al., Deaths among humanitarian workers, in: British Medical Journal 321, July 2000. (www.reliefweb.int/library/documents/Deaths_Among_Humanitarian_Workers.pdf)

Slim, Hugo, Planning between danger and opportunity: NGO situation analysis in conflict related emergencies, January 1996. (www.jha.ac/Ref/ro13.htm)

United Nations, Report of the Secretary General on the Safety and Security of United Nations Personnel, October 2000. (www.reliefweb.int/library/documents/SG_Report_A_55_494.htm)

United Nations, Report of the Secretary General on the Safety and Security of Humanitarian Personnel and Protection of United Nations Personnel, August 2002.

United Nations Security Coordinator, Guidelines for UN/NGO/INGO Security Collaboration, February 2002.

B) Documents and material used provided by aid organisations

Arbeitsgemeinschaft für Entwicklungshilfe (AGEH), Wichtige Hinweise für AGEH-Fachkräfte: Verhalten in Krisenfällen.

Care International, Safety & Security Handbook.

Caritas International, Security Guidelines Kabul, August 2002.

Caritas International, Sicherheitsleitfaden.

Catholic Relief Services, CRS Personal Security Guide.

Deutsche Welthungerhilfe (German Agro Action), Sicherheitsleitfaden, Bonn 2002.

GOAL, Goal Security Policy, August 2002.

Deutsche Gesellschaft für Technische Zusammenarbeit (GTZ), Merkblatt Nr. 9: Krisenbereitschaft, Spannungs- und Krisenfälle, Eschborn 1998.

Handicap International Belgium, Security Guidelines.

Handicap International France, Security Guidelines Sierra Leone.

International Committee of the Red Cross (ICRC), *Staying Alive. Safety and Security Guidelines for Humanitarian Volunteers in Conflict Areas*, Geneva 1999.

International Committee of the Red Cross (ICRC), Head of Delegation Security Package.

International Federation of the Red Cross and Red Crescent Societies (IFRC), Basic Security Awareness.

International Federation of the Red Cross and Red Crescent Societies (IFRC), Security Guidelines.

InterAction, InterAction Security Planning Guidelines.

International Rescue Committee, Security Management Plan Workbook, October 2000.

Malteser Hilfsdienst, *Work Regulation: Use of Malteser Vehicles*, Kampala 2000.

Médecins Sans Frontières, *General Security Framework*, Amsterdam 1994.

United Nations, *Security in the field: Information for staff members of the United Nations System*, New York 1998.

VENRO, *Empfehlungen für den Versicherungsschutz von Auslandsmitarbeitern/innen in der humanitären Hilfe*, Bonn 2000.

World Vision International, *World Vision Security Manual*, Geneva 1999.

Annex 2: Internet sources

Website of the Reliefweb on the safety of staff working for humanitarian organisations:
www.reliefweb.int/ocha_ol/civilians/security_personnel/index.html

Website of the Reliefweb on training programmes in the emergency aid sector:
www.reliefweb.int/training

Bibliography on the topic of staff security:
www.uia.org/surveys/ngohaz/ngosecbi.htm

Website of the Overseas Development Institute's Humanitarian Practice Network:
www.odihpn.org.uk

RedR training programme on security, staff and project management in humanitarian assignments:
www.redr.org

Bioforce security training programme:
www.bioforce.asso.fr

CINFO training programme on security and stress, preparing for an assignment abroad:
www.cinfo.ch

Red Cross information on international humanitarian law
www.drk.de/voelkerrecht/index.htm und www.icrc.org

Annex 3: Organisations and institutions that have been consulted

ADRA

Médecins du Monde

Médecins sans Frontières (MSF)

Arbeiter-Samariter-Bund

AT-Verband

Cap Anamur

CARE Deutschland / CARE International

Caritas International

Diakonie Katastrophenhilfe

Federal Ministry for Economic Cooperation and Development (BMZ)

Federal Ministry of Defence

Foreign Office

German Agro Action / Deutsche Welthungerhilfe (DWHH)

German Foreign Office

GOAL Ireland

Deutsche Gesellschaft für Technische Zusammenarbeit (GTZ)

Handicap International

HELP

InterAction

International Committee of the Red Cross (ICRC)

Johanniter-Unfall-Hilfe

Malteser Foreign Department / Malteser Auslandsdienst medico international

terre des hommes

Technisches Hilfswerk (THW)

World Vision Deutschland / World Vision International (WVI)