MARCH 2001

HPG Briefing

NUMBER 2

HUMANITARIAN POLICY GROUP

Koenraad Van Brabant
RESEARCH FELLOW

About HPG

The Humanitarian Policy Group at the Overseas Development Institute is Europe's leading team of independent policy researchers dedicated to improving humanitarian policy and practice in response to conflict, instability and disasters.

In Brief

- This HPG Briefing looks critically at the organisational structures, management tools and policies that aid agencies are using, or could use, to improve the overall quality of their safety and security management.
- Although there are encouraging steps forward, there remains an urgent need to develop competence rather than just raise awareness among all managers, and for more detailed policy and practice guidelines on specific safety and security challenges.
- It recommends the development of an organisational management plan, as a useful tool to drive a qualitative jump in organisational safety and security management.

odi

Overseas Development Institute

111 Westminster Bridge Road
London SE1 7JD
Tel: +44 (0) 20 7922 0300
Fax: +44 (0) 20 7922 0399

ODI email: odi@odi.org.uk
HPG email: hpgadmin@odi.org.uk
Website: www.odi.org.uk

Mainstreaming Safety and Security Management in Aid Agencies

Although globally it may be commercial company employees and tourists who are most at risk of being killed or kidnapped, in recent years the security of aid agency staff has become a concern for agency managers and their donors.[1] The fact that increasingly they find themselves working in violent environments, together with the perception that they are being targeted have spawned a range of internal measures in a number of aid agencies, and some interagency initiatives.

Is there a need for change?

Problematically, however, in a number of aid organisations, improvements are being delayed by arguments against prioritising and investing in better safety and security management. The most common arguments against are: 'We are not in the emergency or the life-saving business'; 'We haven't had any deaths in the organisation'; 'Risk is an unavoidable part of our work' and 'We have been managing risk for decades with existing tools and competences, there is no need for additional or new measures'.

These arguments reveal dangerous assumptions:

- That the level of risk has remained the same over the past three or four decades.
- That the only risk that counts is that to the life of (international) staff.
- That no deaths in the past is a guarantee for no deaths in the future.
- That risk is only high in actively violent conflict zones, and therefore mainly concerns agencies with an emergency response mandate.
- That risk cannot be reduced through individual and organisational measures.

These assumptions go against the available evidence and analysis which indicate that the number of incidents is on the rise with crime now accounting for perhaps 50 per cent of all incidents, that more agencies are working in danger zones and that the overall respect for them, and therefore for the 'immunity' of their staff, has significantly declined in recent years.

There is furthermore a perception, prevalent also among field staff, that giving too much priority to staff safety and security will create constraints on the fundamental mission of the organisation, which is to provide assistance to people in need. There is indeed an incompressible element of risk in humanitarian aid work, but good security management is also a tool to help agencies enter, and remain in

danger zones, while the loss of assets and especially staff, through accident or incident, impairs the ability of the agency to provide assistance. At higher organisational levels, such laudable emphasis on being operational can also hide an institutional self-interest in market share, visibility and cash flow, at the expense of staff safety and security.

Recent research, based on consultations with 20 agencies, has provided an opportunity to review what organisational steps are being undertaken to improve safety and security management, what has worked well and what less well and why, and where more focused efforts might continue to be required. This paper summarises the main findings[2].

What management tools can be used?

Effecting organisational improvement requires a forum at headquarters where the discussions can take place. An *ad-hoc* working group can do the job but the question arises: what happens when it dissolves? That problem can be overcome by a standing working group on safety and security, to drive the organisational initiatives and monitor their implementation. For it to be effective, senior management needs to be represented on it. Organisations that have achieved a strong safety and security culture can rely on regular senior management team and operations team meetings. But the attitude of the executive director remains crucial: 'safety and security does not start with the type of staff member you recruit, it starts with the type of chief executive officer you recruit' as one aid worker put it.

A common understanding needs to be created around 'safety' and 'security' and what security concept is appropriate for aid organisations. Safety (accidents and health) and security (acts of violence) can both be subsumed under the concept of 'risk management'. But while there is significant complementarity between measures to improve safety and measures to improve security, they are not identical, and focusing only on one or the other would leave dangerous omissions. After an initial emphasis on security, staff safety is now gaining renewed attention. Equally important, however, is the understanding by senior management of what would constitute an appropriate 'security concept' for an aid agency (see Box 1).

BOX 1: Different organisational security concepts

A corporate security concept: Security here has connotations of site protection, protection of confidential corporate information, VIP protection of executives and protecting the organisation from liability through insurance and legal clauses.

A technical-defensive security concept: This has connotations of protective procedures (no-go areas, curfew times, convoy driving, checking-in of visitors) and protective devices (helmets, flak jackets, barbed wire, radios).

A multi-dimensional security concept: This is much more holistic and brings into play the values and principles of the organisation, its mandate and mission, contextual analysis and scenario monitoring, positioning among and relating to a multitude of actors in a particular context, the nature and design of the field programmes and the way the organisation manages all of its staff.

Few agencies currently have a safety and security policy. An argument against is that developing policy creates more bureaucracy. But there are more powerful arguments for putting things on paper: a stated policy makes safety and security management a corporate responsibility rather than an operational issue. It then obliges management to act, and legitimises the allocation of staff time and other resources. It also reduces inconsistency in organisational practices.

A key management question will be how to finance improvements in safety and security? There are some direct costs: insurance, equipment, training and staff salaries constitute the major budget lines for safety and security expenditure. Other costs, such as mainstreaming safety and security in the staff assignment cycle (see below) are marginal. Only a few organisations have already reached the point where safety and security expenditures are habitually written into operational budgets. Even then, some reserve fund will have to be kept at headquarters to cover unexpected and non-budgeted requirements, and some headquarters capacity will have to be covered from core funding. Many agencies have found donors to be fairly receptive to funding security requirements, although wider awareness-raising among the range of donors is still required. At the same time there have been instances where agencies perceived some donors to be making a link between security and funding, as leverage for influencing where agencies can and cannot go. Agencies rightfully resist such 'politics of security', whether by institutional donors or by host governments. But such assertion of agency independence cannot be an excuse not to manage the safety and security of staff in a professional way and donors can legitimately ask potential operating partners to demonstrate that they have that competence. At the same time, staff safety and security are also a direct concern for donors with their own field personnel, such as the US DART teams, the ECHO correspondents, the Swiss Disaster Relief Corps and the UK's Crown Agent operations.

Improved safety and security management, however, also bring 'savings', possibly on the cost of insurance premiums, assets preserved rather than lost, accidents and incidents avoided or having reduced impact. The perceived trend is also for legislation about employer's responsibilities becoming more demanding, and more litigation from former aid workers or their relatives. The cost-benefit calculation therefore seems to be changing in favour of more investment in safety and security management.

A useful tool is an organisational safety and security review. This can be conducted by in-house staff or by external consultants. It will only be effective if there is top-level management commitment to follow up on the recommendations.

BOX 2 Suggested content of a security policy

General introduction, definitions and basic principles:

- a general statement acknowledging risk in aid work;
- a clarification of what is meant by safety and security;
- a general statement that individual staff members and the organisation have a responsibility to try and reduce risk, and that the organisation commits itself to do so;
- basic principles in the organisation's philosophy and practice with regard to security management (the pillars of its safety and security philosophy and practice);
- a statement on the weighting of potentially conflicting objectives, e.g. assisting people in need versus security; witnessing/public advocacy and security; gender policy and security policy; the security of personnel versus that of assets; and
- the status of the document.

Basic principles in the relationship to external actors:

- a statement on the basic position of the organisation towards national laws and local culture and customs;
- a statement of basic principles that will inform the organisation's position with regard to the national authorities, armed protection and the use of private security companies, as seen through the lens of safety and security; and
- exception clauses to the previous paragraph on the basic position, indicating who is authorised to agree a departure from it in special cases.

Basic principles in the relationship between individual staff and the organisation:

- A statement on the responsibilities and freedoms of individual staff members, notably with regard to the right not to go into a danger zone or to withdraw themselves from such without prejudice to their careers; the obligation to adhere to the personal code of behaviour; the obligation to report incidents and to alert other agencies to potential threats; the mandatory nature of security guidelines and disciplinary action in case of breach.
- A statement on the responsibilities and obligations that the organisation accepts with regard to the security of their staff, referring to:
  - a commitment to include a risk assessment in any general assessment;
  - who decides on going into/returning to a danger zone;
  - who decides on withdrawal from a danger zone;
  - a commitment to develop competence in security management/incident survival;
  - the need for security planning and crisis preparedness;
  - the responsibility of management, and the fact that tasks can be delegated but not responsibility;
  - a commitment to incident analysis;
  - a commitment to provide insurance cover;
  - a commitment to manage stress (also cumulative stress);
  - a commitment to provide full medical and psycho-social support;
  - the extent of the organisation's commitment in case of arrest, abduction, sexual assault to the staff member concerned and his/her family;
  - the extent of the organisation's commitment to nationally recruited staff.

As a rule, guidelines should be separated from a policy statement.

What management structures are being used?

Three types of managerial set-up for strengthening safety and security are in vogue:

- the management-line model, where safety and security are located, with other general management responsibilities, within the operational-line management between headquarters (HQ) and the field. A frequent problem for line managers here is the lack of time and sometimes of sufficient competence;

- the specialist security officer model, where one or more such posts are created at headquarters and in the field, often outside and subordinate to the line management. A frequent problem here is the lack of interest or competence among line managers, who can ignore or override the 'advice' of a security officer;

- the security adviser model, where the responsibility for security management lies within the management line, but where there are one or more security advisers at HQ level, who play a proactive and reactive support role for the organisation as a whole, and for specific field offices.

Security expertise in headquarters is usually located in the operations department, although in multi-mandate agencies it is often found in the emergencies or disaster response departments. The latter should be questioned. Safety and security risks may be highest in conflict areas, but are not absent from 'developmental' situations. Landmines and unexploded ordnance, for example, can remain a threat

decades after a conflict has ended, and not infrequently there is a higher incidence of crime in so-called 'stable' situations. Complementing the security expertise may be a health and safety officer. Such a post is more often located in the human resources department, although there are organisations that put this post, together with in-house stress counsellors, also in operations. The human resource department has a very important role to play in ensuring safety and security standards in the organisation, and needs to be actively involved.

Good safety and security management requires clarity about authority and responsibility, the lines of communication and decision-making. Good practice holds that authority and responsibility are vested in line managers, and that safety and security are managed 'close to the ground'. Decentralised organisations are at risk, however, of losing overall organisational consistency, and the checks-and-balances function of HQ. At field level, not infrequently, safety and security-related tasks are delegated to other staff, notably logisticians, a field security officer or administrators. Such delegation of tasks, however, should not result in an abdication of responsibility by the head of the field operations. The more 'focal points' on safety and security there are in HQ and in the field, in principle to support the line managers, the more important it then becomes to maintain streamlined communications, so that managers can retain the overview and the responsibility for decisions.

How can personnel management be improved?

Aid organisations are beginning to acknowledge more formally their general responsibility for the safety and security of their staff. Spelling out the detailed commitments of the organisation, particularly also where it comes to staff members that are victims of kidnapping or sexual aggression, or who become disabled as the result of accident or incident, will increase staff trust and loyalty to the organisation. Attention in any case must be paid to evolving legal requirements of employers, and to legislation relevant to national staff. It is doubtful that making staff sign a statement that they will not hold any claims against the organisation in case of incident or accident is morally and legally defensible.

At the same time, some organisations are also clarifying their expectations of individual staff members. In principle, staff have the liberty to refuse to be deployed in a risk zone, but repeated refusals would also suggest that the individual and the organisation must part ways. Organisations are also increasingly stressing that observance of security rules is mandatory and that breaching them can give rise to disciplinary action, including obligatory repatriation. A fairly recent development is the clarification by several agencies that staff members need to behave responsibly and respectfully 24 hours a day and seven days a week, and not just during office hours. Personal behaviour can directly (for example, drunken driving) or indirectly (for example, provocative arrogance, cultural disrespect, bringing prostitutes into the premises) put at risk the staff member or colleagues, or may negatively affect the image and reputation of the organisation. Some organisations are now formalising this in a code of personal behaviour. The scope and formulation of such a personal code will be a discussion point for management.

Increasingly safety and security consciousness is being introduced in the various steps of the assignment cycle. Explicit enquiry and testing of applicants about their attitudes to risk and risk management can be introduced in the recruitment process, including recruitment of candidates for senior staff positions. Agency policies, practices and expectations on safety and security can be addressed in an induction course. Pre-departure briefing and in-country arrival briefing for international staff should cover the context, the general pattern of threats and risks and the risk-reduction measures in place. Some agencies have decided to be very open about the risks that staff members may face. At any stage in the assignment, staff members retain the liberty to withdraw if they feel that the risk is more than they can cope with. Post-deployment or end-of-contract debriefings, for international but also for national staff, are an opportunity to check the individual's well-being, but also to learn from such feedback on the organisational management of risk.

Many surveys confirm that staff experience stress as a major concern. In the organisational responses so far, however, the emphasis is often more on the more visible post-traumatic or critical incident-related stress than on cumulative stress which can lead to burn-out. There is also very limited awareness, let alone attention to, perhaps significant cultural differences in the experience of stress and approaches to stress reduction.

Unfortunately the fact remains that the safety and security of national staff in general remains a conspicuous weakness, compounded by a resistance to face the issue. Clarity of thinking is not helped by the automatic association — and reduction — of that concern to the issue of evacuation. This can make agencies overlook the fact that national staff also face health and safety hazards, and can be at risk from landmines, armed robbery, ambush, hostage taking and sexual assault. Given that the global trend in staffing is for more national and fewer international staff, a change in attitude and more constructive thinking are urgently required. Among the more progressive practices already being adopted are more detailed vulnerability and risk analysis, differentiation between international and national staff and categories of national staff; insurance cover and training opportunities for national staff as well, and the articulation of basic policy principles that confirm the responsibility of the organisation to care for their national staff where these face risk or suffer because of their work. Some organisations also offer social benefits for national staff who suffer accident or incident.

What operational reinforcements are required?

The necessity to carry out risk assessment as part of the very first needs assessment, prior to going into or returning to a danger zone, is gradually being recognised. This marks a slow

change in organisational culture with risk awareness and risk management introducing some caution into a sector with a competitive and action-oriented mentality, where all caution is sometimes thrown to the wind. Most agencies recognise that their competence at risk assessment remains very limited.

The security plan has historically been the pillar of the security management of many aid agencies. In practice, its production often mainly fulfilled an administrative requirement and the plan remained a dead document with little effective reduction of risk.[3] Having identified the problem, more agencies are now developing guidelines for security planning against a generic template that needs to be adapted locally, putting more emphasis on the planning process and on a team approach. Those most advanced in security management, however, see the security plan only as one tool among many. Maintaining alertness, active monitoring of the environment, proactive scenario thinking, analysing incidents, strengthening of awareness, competence and discipline are other important components. The emphasis is on a management plan for security, at HQ and at field level, rather than on the security plan.

In only a few agencies are HQ staff confident that they know about almost all incidents. The most common view is that HQ is likely to hear about serious incidents, but by no means all. And in quite a few agencies there is considerable under-reporting. There are obstacles to incident reporting that are more related to the individual, but there are also disincentives against reporting in some organisations. The most common ones are concern about subsequent HQ interference in the programme or damage to one's career prospects if an incident is seen as management failure. If there is room for improvement in incident reporting, there is a major gap with regard to incident analysis. While this offers the best learning opportunity, it is seldom done and even then rarely documented. Equally problematic is the sharing of incident reports between agencies. This seems a minimum obligation for the purpose of sounding the collective alert, but obtaining a fuller picture on security incidents is necessary for proper threat and risk assessment.

Safety and security measures reduce risk, but cannot of course fully eliminate it. So 'crises' may occur. Some organisations have thought through their crisis preparedness, but others have yet to identify who would or should participate in a crisis management team at HQ or how certain types of crisis should be managed. Steps towards better crisis preparedness would include: a clear definition of what constitutes a crisis, 24-hour communication with HQ through a system of:

- duty officers who are clear about the parameters of their decision-making authority;
- the proactive identification of core members of a crisis management team (with identified substitutes in case a member is unavailable); and
- some training of the crisis management team with role plays and simulations.

There are generic characteristics of crisis management, but also specifics depending on the type of incident. Recently, the risk of kidnapping has drawn considerable attention, and several agencies have called on external expertise for advice on how best to manage such situations. In contrast, sexual assault and rape remain largely neglected, although there must be as many, if not more, of these incidents. There is significant confusion about the management of this latter threat and of such incidents, which is not helped by treating the risk as a taboo or adopting an attitude of 'what can be done about it?'. Where the risk is beginning to be acknowledged the management responses frequently approach it from another angle: in the context of sexual harassment or as a type of traumatic incident for which counselling is offered. This is grossly inadequate. Field managers need to be given practical guidance on immediate rape response, which will have to take place before any professional post-traumatic incident counselling can be mobilised.[4]

Safe sex, to protect staff from sexually transmitted diseases, is now explicitly addressed by many agencies. Several organisations ensure that condoms are always available to national and international staff in the field, and can be obtained discreetly. For some religious organisations, this has not been possible. They limit themselves to advising staff to use condoms.

To what extent agency autonomy?

The analysis of security incidents and of practical security management at field level indicates a fair degree of interdependence between agencies. There is significant scope for more interagency collaboration to develop greater competence in safety and security management. Yet the most emphatic message of aid organisations is their insistence on retaining full autonomy. That is legitimate inasmuch as they have the formal responsibility for staff. But it should not blind people to areas where collaboration is possible, beneficial or even actively required.

Although international agencies often work with and through local governmental or non-governmental partners, that relationship, when it comes to safety and security management, has yet to receive focused attention. Existing attitudes range from 'this is not our concern' to 'a genuine partnership requires that we allow them to pursue their own strategies and we are prepared to provide them with capacity-building support'. The issue merits further thought for each given situation, and at a general level.

What factors inhibit or facilitate organisational change?

There is strong convergence of opinion about factors that are felt to be constraints, and those that are experienced as facilitating the improvement of safety and security management. The most important inhibitors are: lack of interest and commitment in top management; an

organisational culture with either excessive voluntarism or excessive bureaucracy; excessive operationality with nothing in writing; a competitive orientation that encourages risk-taking behaviour, or a self-congratulatory attitude that disregards failures and weaknesses; excessive centralisation but also excessive decentralisation in the structure; a shortage or misuse of expertise; organisational and team instability; excessive workloads; and complacency because few staff and managers are confronted with high-risk situations.

The most effective facilitating factors are active interest and commitment among top management; an organisational culture of care for staff, support for learning and attention to realities on the ground; an organisational structure without too many layers of management; effective fora for discussion, policy development and decision-making; the availability of staff who can stand back from the day-to-day pressures to reflect and think strategically; internal triggers such as a dramatic incident or a safety and security review; and external pressures from the media and evolving legislation, but also external opportunities such as interagency development of resources and benchmarks.

The size of the organisation and whether it is faith based or not, seems to have little influence on how well safety and security are managed. Factors that do have a strong influence are the mandate of the organisation, the funding base, the layers of management and 'change fatigue' (namely, the impact of restructuring and strategy changes on staff motivation and organisational efficiency). Organisations that work in 'family networks', that work through partners or with a highly decentralised structure, can find that these characteristics complicate the efforts to strengthen safety and security, unless they are well managed.

How to improve policy and practice: a management plan for change

Very few agencies at any point seem to have developed a management plan for the strengthening of safety and security. This may not be necessary once there is a strong organisational awareness and competence. But otherwise it may be a useful tool to drive a qualitative jump at crucial moments of earlier organisational development. A management plan sets out concrete objectives that the organisation wants to achieve within a defined time frame. It sets priorities and becomes the reference for designating responsibilities and allocating staff and financial resources. It will also be the reference for monitoring progress. Ideally, a management plan is based on analysis and objective setting, rather than being built on the (temporary) availability of resources. Developing a management plan is not an easy task, but the exercise itself can be an important step in generating organisational commitment and momentum.

Footnotes

1 Annan, K. 2000: Safety and Security of United Nations Personnel. Report of the Secretary-General. New York, United Nations, General Assembly.

2 Van Brabant, K. 2001: Mainstreaming the Organisational Management of Safety and Security. A review of aid agency practices and a guide for management. London, ODI, HPG Report No. 9 (www.odi.org.uk/hpg).

3 Van Brabant, K. 1997: Security Guidelines. No guarantee for security. London, ODI, RRN Newsletter 7 (www.odihpn.org.uk).

4 Van Brabant, K. 2000: Operational Security Management in Violent Environments. A field manual for aid agencies. London, ODI, HPN Good Practice Review No. 8. Chapter 12 (www.odihpn.org.uk).

The full report on which this Briefing Paper is based is available from ODI entitled: Van Brabant, K. (2001) *Mainstreaming the Organisational Management of Safety and Security*, HPG Report No 9. London: Overseas Development Institute. The full report spells out the arguments in more detail and offers some practical tools for managers. Further information regarding HPG publications is available from: www.odi.org.uk/hpg/publications.html or from publications@odi.org.uk

Overseas Development Institute, 111 Westminster Bridge Road, London SE1 7JD
Tel: +44 (0) 20 7922 0300 Fax: +44 (0) 20 7922 0399 Email: odi@odi.org.uk Website: www.odi.org.uk