Report of the Working Group on NGO Security Training Curriculum

NGO Security Working Group

Jane Swan
InterAction

Santhe Loizos
InterAction

Lucy Brown
American Red Cross

Jan Davis
RedR

Jonathan Dworken
Center for Naval Analyses

Dave Dyck
Eastern Mennonite University, Conflict Transformation Program

Rob Lowe
Cable and Wireless

Michael O'Neill
Peace Corps

Lisa Schirch
Eastern Mennonite University, Conflict Transformation Program

Koenraad Van Brabant
Overseas Development Institute

About this report

In 1995, the U.S. Agency for International Development's Office of Foreign Disaster Assistance (USAID/OFDA) provided InterAction with a grant to develop curricula for non-governmental organization (NGO) training courses in two areas-health and security.

This report focuses on the security training component of the grant. It summarizes the work of the advisory Task Force and Security Working Group, and includes summaries of the following:

- Work undertaken by the project, including development of the curriculum and holding of two pilot courses;
- Unique approaches to security and training adopted by the Task Force and Working Group;
- Learning objectives and modules produced for the course;
- Formal and informal evaluations of the course.

The primary purpose of the report is to describe the work done under the project and to recognize the efforts of the individuals and institutions which have contributed to its success, in particular those of the Working Group that produced the final materials, and designed and implemented the pilot courses.

The larger objective of the report is to document what we have learned about NGO security and security training over the course of the project so that those pursuing further initiatives in NGO security training can build upon what we have done.

Jane Swan
Project Director

Table of Contents

Project Description

OFDA Grant

As part of the review of NGO operations during and after the 1994 Rwanda genocide, NGOs belonging to InterAction worked with OFDA to identify training needs to improve NGO performance. Health and security were identified as the top priorities. In 1995, OFDA responded to these needs by providing InterAction with a grant to develop curricula for courses in both areas. This report summarizes the work of the security component of the project.

Project History

In December 1995 InterAction hired a Project Director and work on the health component of the project was initiated. In July 1996 the first security Task Force meeting was convened, and was comprised of members of InterAction's Disaster Response Committee, as well as recognized experts in security.

Subsequently over the course of a year, NGO members of the advisory Task Force met to determine the focus and approach to security training which would meet the needs of the NGO community. They determined the following about the course:

- The approach should focus on enhancing judgment and decision making.
- The target audience should be those with experience in positions of responsibility for field security.
- It should be limited to a week.
- It should include a train-the-trainers component.

In mid-1997, consultants with specific areas of expertise were engaged to write the curriculum and design the course. The Project Director and Associate, one Task Force member, and the consultants became the security training Working Group which developed the course modules and piloted the courses held in January and September 1998.

Project Outputs

Under the grant, there were two types of outputs-written materials and pilot courses. First, the Working Group developed the following written materials:

- A series of modules that comprise the curriculum. These were provided to course participants as reference material, and most were used in the courses.
- Exercises and accompanying lesson plans.

At the end of the project, the course modules, exercises and lesson plans were provided to USAID/OFDA.

Second, two one-week pilot courses on NGO security were held. In each course, there were 25 participants from operational NGOs, the majority of whom were currently working in the field. Both courses required agency sponsorship to attend, and had more applicants than could be accommodated.

- The January 1998 course was held in Flamingo, Florida USA, and included a train-the-trainer component. Sixteen agencies and seven nationalities were represented.
- The September 1998 course was held in Bedfordshire, England in order to facilitate the participation of field staff and European NGOs. Eleven nationalities representing twenty-two agencies participated. There was no train-the-trainer component.

Project Impact

While difficult to measure, the Working Group believes the project had impact in the following ways:

- Trained 50 people in NGO security, many of whom went on to hold training courses for their organizations and others in the field and/or implement improved security measures within their organizations.
- Developed course modules and lesson plans that others could build upon for developing resources for security management and future training. Thus far, one NGO has included material developed for the course in a newly published field guide, and one European training organization is using the curriculum for the security courses which it offers to NGOs.
- Provided a framework, language and forum for dialogue which may contribute to a more sophisticated approach on the part of the relief community to security challenges. The unique, NGO-specific approach taken is discussed in the following section.

Course Approach

The Task Force and Working Group had a unique approach to NGO security which, in turn, had a significant impact on the approach taken to training on security.

Approach to Security

In developing the course, the Task Force and Working Group developed a unique approach to security. Initially, participants in the Task Force meetings looked at approaches to security based on those used by diplomats, corporations, and militaries. These approaches often stressed the importance of personal security, standard operating procedures (SOPs), and technical approaches to improving security.

After considerable discussions, however, it became clear that this traditional model was not *completely* applicable to the NGO community given its unique mission. NGOs have very particular values, limited resources, and a need to interface with the community to operate effectively. These characteristics make it difficult and inappropriate to rely upon an approach to security that requires significant resources, further isolation from the community, and the threat of force. NGOs participating in the Task Force and the Working Group, as well as those interviewed for this project in Europe and Africa, expressed the need for something different.

The Task Force and Working Group, therefore, gradually developed another model that might be described as a holistic view of "NGO security management," the major components of which are as follows:

- *Relationships*. Traditional approaches to security which focus primarily on "personal security" may underestimate the interdependence of security and relationships. Many relationships play a key role in improving security: healthy personal relationships within an NGO allow teams to act together rapidly with mutual confidence in a crisis; within the NGO community, positive relationships contribute to trust that allows for sharing of sensitive security information and coordinated responses to threat; and good relationships with the local populace will foster communication and may prevent resentment and hostility.
- *Agency- and situation-specific approaches*. Approaches to security that provide prescriptive "one-size-fits-all" SOPs may not be appropriate or useful. Situations differ as to the types and degree of threat. Agencies differ with regard to their principles, activities, risk propensity, and capability and willingness to use specific measures, such as armed protection. These differences must be reflected in the security practices they adopt.
- *Analytical skills and decision making*. To move beyond a prescriptive SOP and make informed, situation- and agency-specific security decisions, NGO field leadership needs tools and conceptual frameworks to further refine their analytical skills and judgment on security issues. Effective security management requires analytical skills to assess the context, threats, and agency vulnerabilities; to

develop appropriate security strategies based upon this assessment; and to evaluate and modify strategies and plans as the situation changes.

- *Strategy*. Depending on the specifics of a situation and the NGO, there are a variety of strategies to improve NGO security: acceptance (building relationships), protection (procedural and technical measures to reduce exposure), deterrence (counter-threats, such as armed protection), or some combination thereof. Different strategies are effective in different circumstances, and an approach which enhances security in one situation may contribute to greater risk in another.
- *Strategy-based security plan*. A security plan includes SOPs and contingency plans (e.g., for evacuations). If a plan is written without specifically developing and articulating a security strategy, it may result in conflicting practices, such as when an agency wants to improve relations with a local populace, but the staff adopts security measures that send a signal of distrust. By basing SOPs and contingency plans on a specific security strategy, NGOs can often avoid this problem.
- *Multi-disciplinary approach*. To develop and adopt this broad approach to security management, NGOs must work together to identify undocumented good practices, draw appropriately from the traditional security experts, and reach beyond these experts to gain insights from other disciplines (e.g., area experts, conflict transformation specialists, researchers, and analysts). Few of the individual components of this NGO security management model are unique. When taken together, however, they provide a unique, NGO-specific, holistic approach to security that has not previously been articulated.

Approach to Training

This approach-NGO security management-led the Working Group to develop an approach to security training with the following key components:

- *Selection of participants with experience and in positions of leadership*. Almost all of the participants held positions in which they had some responsibility for security. This allowed them to draw upon and share experiences in a constructive manner that maximized individual and group learning. That participants were in leadership positions helped insure that the course would have a larger impact; they would be able to disseminate and implement what they had learned upon returning to their organizations.
- *Adult learning methodology*. To maximize learning, trainers used a mix of techniques which drew out and built upon the knowledge and experience of the participants, including lectures, facilitated group discussions, case studies, exercises, role plays, simulation, hands-on demonstrations and practice, videos and slides.
- *Integration of training and research*. Because there are so few documented NGO-specific good practices in security, research was conducted in conjunction with the courses. There was an opportunity for participants to learn from the

experiences of one another, and also for the Working Group to begin to identify good practices by drawing upon the experiences of the participants.

- *Diversity of perspectives*. Recognizing the diversity of views on security issues and the importance such diversity contributes to a more complete and accurate understanding, participants were sought from different backgrounds, agencies, countries, gender, parts of organizations (headquarters and field staff), and status (expatriate and national staff).
- *Linking the conceptual and practical*. Tools and conceptual frameworks were developed to enhance the analytical skills of participants. Trainers used case studies, practical exercises, and facilitated group discussions to demonstrate the utility of the tools, and to train participants in how to use them.
- *Field demonstrations and hands-on practice*. Course locations were selected which allowed for role plays with vehicles and checkpoints, demonstrations and practice using telecommunications equipment, and practical exercises including methods for extricating oneself from a minefield.
- *Single scenario*. In addition to real case studies, trainers used a single scenario of a fictitious country called "Flamingor." Using the same scenario for different exercises throughout the course reduced the time spent doing background reading on a situation, and allowed for a common understanding of a situation to develop. This in turn permitted participants to quickly focus on the purpose of an exercise, such as understanding the impact of NGO security measures on how you are perceived by the local population.
- *Final simulation*. In a final simulation using "Flamingor," participants were required to implement an evacuation plan they had written the previous day, as well as practice many of the skills learned throughout the course.
- *Train-the-trainers*. In the initial pilot course, there was a training-of-trainers component which included development of training skills and the opportunity to prepare to provide security training to others in the field.

Course Summary

The courses were based on the specific approaches to security and training adopted by the Task Force and Working Group.

Overview

The course design was based on a structured approach to NGO security management. There were four core components that were adapted from the traditional management cycle.

- *Assessment*. Assessment of the situation, including the context, threats to NGOs, vulnerability to those threats, and risks.
- *Planning*. Adoption of an appropriate security strategy and the process of developing a security plan, which includes appropriate SOPs and contingency plans.
- *Implementation*. Knowledge and skills-procedural, technical and behavioral-needed for effective implementation of a plan, including both preventive measures and response to incidents.
- *Evaluation*. Analysis of security incidents to re-assess the situation and the effectiveness of your security strategy and plan.

Many topics covered in the courses were cross-cutting, and pertinent to all aspects of the management cycle. Some of these were addressed in written modules, while others were discussed as they arose during the course, such as relationships between headquarters and the field, and between expatriate and national staff.

Module Summaries

The Working Group produced a series of course modules which were provided as reference material to the participants. Given the time constraints, not every aspect of each module was discussed during the course.

The following pages provide brief descriptions of the modules-both those relating to the four core components above and those focusing on cross-cutting issues. The descriptions are a synthesis of the written modules and what was taught in the courses, and are therefore not identical to either.

1. Re-thinking NGO Security: A Systems Perspective

Goal: To provide an analytical framework for thinking about NGO security.

Objectives:

- Understand the significance of security crises in a larger framework.
- Introduce a systems framework that (1) helps to situate security crises/incidents within a broader framework of relationships and systemic factors, and (2) demonstrates how immediate responses to crises and mid-range policy decisions have significant implications for long-term mission and security strategy, and vice-versa.
- Introduce the concept that work is required both within an organization and between an organization and its surrounding communities to decrease vulnerability.

Summary: The current attention to NGO security provides an opportunity to re-envision larger questions of NGO projects, mission statements, and procedures. It is important to analyze security incidents and place them in their broader context. Crisis events are inevitably embedded within a longer perspective of time and a more complex set of relationships. A crisis and incident requires a response, but so do the root causes of the crises. The decisions made and actions taken in response to an immediate crisis will have significant implications for NGO vulnerability in the long term.

2. Image and Acceptance

Goal: To enable an agency and its personnel to act in a manner which enhances acceptance of its presence, and to understand how such acceptance contributes to security.

Objectives:

- Understand your agency and how others perceive it.
- Differentiate between groups which perceive your agency in different ways.
- Determine factors which contribute to agency image.
- Identify ways in which a discrepancy between what an agency tries to project and how it is actually perceived may affect security ("image gap").
- Develop strategies which enhance acceptance and reduce the "image gap."

Summary: The way an agency and its personnel are perceived has an influence on security. Resistance to your presence may increase risk. NGO image is derived not only from the messages NGOs consciously communicate, but also from those unconsciously communicated. The way NGOs are perceived by others may be different than the way one thinks, and this may affect security. NGOs should question staff appearance, behavior and roles, as well as seek feedback from others as to how the NGO is perceived. NGOs must recognize and differentiate between groups which may perceive them in different ways, and manage personal behavior in ways which gain acceptance.

3. Power, Image, and Security

Goal: To explore how power and the images that portray power affect security

Objectives:

- Explore the relationship between power and security.
- Increase the awareness of how power is used in NGO contexts.
- Understand how power can be used effectively without threatening others.

Summary: Disparity in power is a dynamic in many conflicts and security problems. People tend to feel disempowered and threatened when others around them appear to clearly possess more power. People feeling insecure or threatened are more likely to use violence to gain a sense of power (nothing hides a whimper better than a growl). Awareness and analysis of your own power, and your ability to use it in ways that are assertive without threatening others, will increase your security. Individual NGO personnel and NGO organizations, as a whole, can make a conscious choice to divest themselves of some of the symbols which serve to emphasize the differences in levels of power between them and the local community. Adopting a team philosophy which emphasizes humility and the need to listen to, learn from, and often defer to local people and customs can dramatically reduce overall aggressiveness towards the NGO.

4. Legal Framework and Protection

Goal: To increase protection for civilians and NGO personnel through an understanding of the legal framework of protection and through an introduction to protection strategies.

Objectives:

- Describe the usual legal status of NGOs in the field under International Humanitarian Law (IHL).
- Explain why impartiality and consent may be crucial for the protection of NGOs providing humanitarian assistance.
- Describe options available to NGOs in responding to humanitarian or human rights violations, and the accompanying security considerations.
- Identify three strategies for the protection of civilians at risk.

Summary: Under international humanitarian law, NGOs usually receive only the general protections accorded the civilian population, and are not entitled to provide humanitarian assistance unless they first meet the twin requirements of impartiality and consent. Those acting without meeting these requirements must seriously consider the increased security risks for themselves and others. NGOs must determine what role they should play along the "protection continuum," and ask whether the accompanying security risks will be acceptable.

5. Security Strategies

Goal: To provide a conceptual framework for developing strategies for security management.

Objectives:

- Describe three strategies for security management.
- Articulate advantages and disadvantages of each strategy.
- Indicate the factors to consider in determining which strategy to adopt.
- Articulate which strategies are most effective for which types of situations and threats.

Summary: Effective security management involves finding the most appropriate mix of strategies in any given (and changing) situation. There are three potential strategies: (1) acceptance as a strategy refers to that which an agency or individual does to enhance security through building positive relationships; (2) protection refers to the use of procedures and protective measures to reduce vulnerability to threat; and (3) deterrence refers to the use of counter threat, including sanctions and armed protection. Different strategies are effective in different situations-a strategy which enhances security in one situation may reduce it in another. A complete understanding of the situation, and the complexity and dynamics of employing a mix of strategies, is crucial.

6. Armed Protection

Goal: To provide an overview of the considerations which inform policy and practice concerning the use of armed protection.

Objectives:

- Articulate the principles which inform a decision to use armed protection or not.
- If an agency would consider the use of armed protection, articulate under what conditions and for what purposes.
- Articulate how the use of armed protection impacts how the agency is perceived.
- Articulate the advantages and disadvantages of using different providers of armed protection.
- Articulate key issues in the management of armed personnel.

Summary: There is not consensus concerning whether the use of armed protection is appropriate as a deterrent strategy for NGOs, and if so in what circumstances. A decision to employ armed protection has an impact on the image of the agency as well as on the image of other agencies with which it is linked, either formally or informally. If armed protection is used, it must provide a reasonable deterrence to specific threats and be well managed, as the use of armed protection may have the opposite effect and actually increase the risks.

7. Context Assessment

Goal: To provide a framework to analyze the contextual aspects of the environment which impact security, either directly or indirectly.

Objectives:

- Articulate the political, social, economic, geographical and cultural components of a regional/ country profile.
- Articulate the different components of conflict analysis, including the causes, participants and dynamics.
- Determine the political economy of a conflict and how the agency presence and programs might impact or be impacted by it.
- Articulate how an understanding of context can impact security and the potential risk of being targeted.
- Identify possible sources of information and their respective advantages and limitations.

Summary: A country profile provides the foundation for security management, as well as for effective program planning and development. In situations of conflict, an understanding of the conflict (including the motivations, resource base and shifting relationships between those involved) is vital. It is possible to reduce the likelihood of becoming a target through effectively managing the potential impact of agency operations on the conflict. Accessing a variety of sources for information, and taking into account the potential bias and limitations of each, will help you develop a more accurate view of the context.

8. Threat Assessment

Goal: To improve the ability of NGO staff to assess threats to NGO personnel and property, thereby helping to make more-informed decisions about which security strategies, procedures and plans to adopt.

Objectives:

- Articulate the link between threat assessment and security measures.
- List the types of information you want to get from a threat assessment.
- List three causes of threats.
- List four general approaches to conducting threat assessments.

Summary: A threat is any event that may result in harm or injury to NGO personnel or loss or damage to NGO property. Threat assessment-the analysis of the likelihood that NGOs will confront threats-helps NGOs make more-informed decisions about which security measures to adopt. It does so by identifying the most likely threats NGOs will face, allowing identification of the security measures most likely to keep NGOs safe-and avoidance of unnecessary measures. Threat assessment is not a one-time event, but a process of continuous re-evaluation of threats to ensure that you continue to have appropriate security measures in place. Techniques for threat assessment include: interviews, analyzing patterns and trends, gauging the threat level, and looking for indicators that threats may change. Each approach has its own strengths and limitations. It is therefore important to use all four together to conduct a threat assessment.

9. Vulnerability and Risk Assessment

Goal: To understand factors which make one more vulnerable to threat in order to reduce the risk, or likelihood of threat by altering those factors which can be altered to prevent or mitigate the harmful effects of threat.

Objectives:

- Define and articulate the link between threats, vulnerability and risk.
- List factors affecting your vulnerability.
- Identify factors which make threats serious and how therefore to reduce the risk.

Summary: Threat is the possibility that someone will harm NGO personnel, or steal or damage NGO property, through purposeful, often-violent action. Not all NGOs are equally vulnerable to those threats. Vulnerability-the extent to which an NGO is susceptible to threat-differs among NGOs because vulnerability is based upon the location of NGO staff and property, exposure of NGO personnel and property, value of NGO property, impact of NGO programs, adoption of appropriate security measures, compliance of staff with security measures, staff interpersonal skills, and the image of staff and programs. Focusing on vulnerability assessments highlights the roles of staff behavior and programming. Risk refers to the likelihood of being affected by threats. The seriousness of a threat is based upon its impact on staff (deaths, injury, and stress, personal belongings) and programs (success in assisting beneficiaries, program continuation), as well as the likelihood of the threat occurring. NGOs can reduce risk by preventing incidents from occurring and by mitigating their effects if they do occur. While there may not be a means of reducing threats, NGOs may reduce their vulnerability and risks associated with threats.

10. Security Planning

Goal: To provide the concepts, principles, techniques and tools to develop a security plan.

Objectives:

- Articulate how an agency's mission, security strategy and threat assessment are incorporated into a security plan.
- Identify who is responsible and should be included in the planning process, and why.
- Outline the steps for developing a security plan.
- Outline the components of standard operating procedures and contingency plans.

Summary: Security planning is a process which should involve all those expected to implement the plan. It is part of the larger security management cycle, and as such should be based upon assessments (context, threats, vulnerabilities, risks), as well as the security strategy of the agency. Security planning is a dynamic process requiring regular evaluation and updating as the situation changes. The purpose of a security plan is to

enable personnel to act effectively to prevent and mitigate the effects of security problems in a manner appropriate to the agency. At minimum a security plan should include standard operating procedures and contingency plans for the most likely contingencies (outlining the who, where, when, and what to do).

11. Site Security

Goal: To enhance the security of residential and work environments so that operational objectives can be achieved with minimal loss and damage to material or injury to personnel.

Objectives:

- Identify factors to consider in selecting a site.
- Identify factors to evaluate in implementing site security measures.
- Articulate how different choices may impact how an agency is perceived.
- Identify potential threats to site security and measures which can reduce vulnerability.

Summary: It is important to select sites and implement security measures which reflect the agency's security strategy. The security of a site is related to the profile of the agency, including its programs, assets and behavior of personnel. A site and its affiliations can influence how an agency is perceived, which, in turn, will impact vulnerability. Site security is generally maintained through a series of physical and procedural boundaries which control access. Effective site security requires that personnel consistently implement the standard operating procedures, which should be regularly evaluated and revised based upon changes in the situation.

12. Vehicles and Movement

Goal: To minimize the risks associated with vehicles and movement.

Objectives:

- Outline standard operating procedures for responsible vehicle management.
- Outline the roles and responsibilities of drivers and passengers.
- Identify measures to take in preparation and planning of a journey.
- Outline standard operating procedures for vehicle movement, including checkpoints, convoy organization, and reporting of incidents.
- Identify measures to reduce vulnerability to threats, including hijacking and ambush as well as responses which mitigate the impact should they occur.

Summary: A vehicle may be an essential working tool and a means of escaping danger. But at least half of all security incidents occur during travel because a vehicle may be a symbol or a valuable commodity which makes it and its occupants potential targets. It is important to have clear, agreed upon and understood guidelines on vehicle use and

management. Vehicles should be maintained in a state of operational readiness, journeys need to be planned, and vehicle users must be prepared to respond to a range of possible incidents. Clarity of roles and responsibilities for all personnel both for standard operations and in the event of contingencies are essential for effective management.

13. Telecommunications

Goal: To provide an overview of telecommunications options and to outline the necessary steps for initiating and maintaining a viable communications network within the NGO environment.

Objectives:

- Indicate the physical properties of HF, VHF, and satellite communication.
- Indicate the advantages and disadvantages of available systems.
- Indicate the criteria that determine the communication needs of an agency.
- Indicate the means to achieve the greatest utility from telecommunications systems currently in place.
- Describe technological advances in telecommunications.
- Outline general guidelines for operation for all networks.

Summary: Without the ability to transfer information between various levels in an agency, as well as among different agencies, an organization may face difficulty adapting to situations which arise. Different equipment has different capabilities. Prior to selection of a system, assess both the immediate and projected needs of the project, as well as systems currently in place which one may utilize or interface with. The human factor is the most vital in any communications network, and the training and discipline required to operate one are an essential component of security management.

14. Self Management to Reduce Vulnerability

Goal: To provide the principles and tools for self management to reduce the vulnerability to threats.

Objectives:

- Identify the different styles of managing conflict, realize which one is your own dominant style, and understand the importance of using different styles depending on the specific situation.
- Identify methods for responding to and managing your own fear and panic.
- Name the components of the arousal cycle, and what responses/characteristics accompany each.
- Identify principles for managing your anger.

Summary: The manner in which one responds to any given situation, crisis or otherwise, has long-term implications for how one is perceived, relationships with others, and your

security. Individuals who are aware of their patterns of dealing with crisis and understand the impact of their style on others are less likely to behave in ways that may escalate crisis. Those who are unaware of or deny their emotions are more likely to have the emotions influence them in destructive ways. Reflection and mental preparation are key in the management of intense emotions.

15. Team Management to Reduce Vulnerability

Goal: To increase team functioning and thereby reduce security risks.

Objectives:

- Identify the characteristics of a healthy team and indicate how such characteristics serve to enhance security
- Indicate how decision-making processes can affect the security of an NGO.
- Explain the different ways to make a decision and articulate a way to determine the most appropriate and security-enhancing method for a given context.
- Explore the manner in which organizations can pursue discipline and accountability in such a way as to promote greater security.
- Articulate the role of gender and its impact on team security.

Summary: When an NGO team functions as an effective group, the security of the team is enhanced. Teams in which each member understands and respects the overall organizational philosophy, their place in the team, and the expectations of them both on a daily basis and in a crisis, are less vulnerable. The primary way to establish healthy group functioning is by ensuring that there is clarity in organizational identity and boundaries, roles, communication, decision-making, conflict management and team building.

16. Preventing and Defusing Anger and Hostility

Goal: To learn how to prevent, defuse and de-escalate security incidents which involve dealing with angry, hostile people.

Objectives:

- Understand how respectful behaviors reduce vulnerability.
- Explore principles which work to redirect and de-escalate aggression.
- Learn specific behavioral approaches and communication skills which de-escalate anger and hostility through nonverbal, listening, and speaking skills.

Summary: Anger and aggression are often borne out of frustration and a feeling of powerlessness. Efforts to resist physically or verbally are often counterproductive, putting the aggressor(s) in an even more defensive position. By using nonverbal and verbal postures that reflect your calm and confident ability to respond and interact with the aggressor, people can learn to use respectful communication to de-escalate and defuse

anger and aggression. The ability to communicate skillfully and appropriately so as to foster acceptance has a great impact on security.

17. Abduction and Hostage Taking

Goal: To reduce vulnerability to abduction / hostage taking, and to be prepared to respond in ways which mitigate damage in the event that abduction / hostage taking occurs.

Objectives:

- Identify measures which reduce vulnerability to abduction/hostage taking.
- Articulate measures to take in contingency planning for abduction/hostage taking.
- Articulate principles for survival if abducted/taken hostage.
- Articulate factors to consider while negotiating for release of hostages and afterwards.

Summary: Motives for abduction/hostage taking vary. Threat assessment should attempt to discern possible motivations as this will guide preventive measures beyond the general protective measures which can be adopted. Management of a hostage situation requires resources and skills which must be anticipated, planned, and prepared for-before a situation occurs. Preparation in advance for what to expect and how to behave should one be taken hostage may serve to mitigate the harm done.

18. Landmines

Goal: To minimize the risks associated with working in places where the presence of landmines is possible.

Objectives:

- Describe types of mines and the ways in which they are triggered.
- Identify precautions to take in an area in which landmines may be located.
- Identify areas likely to be mined (reflected in the reasons for laying mines).
- Identify indications of the presence of mines.
- Describe actions to take on finding oneself in a mine field, or on suspicion of being in one.

Summary: An agency should obtain the help of local expertise to carry out a threat assessment and training when operating in an area which is potentially mined. Obtain as much information as possible before entering an unfamiliar area. Landmines are laid for a reason, and an understanding of the history, context and geography may help to understand which areas are most likely to be mined. Avoid mined areas. If you do find yourself in a mine field, stop all movement, follow prescribed measures for extricating yourself if there is no possibility of outside assistance, mark the mine or mine field, and report the incident in order to warn others.

19. Stress and Trauma

Goal: To describe the process and skills needed to address stress and trauma experienced by NGO workers after a critical incident.

Objectives:

- Describe the expected effects of stress and trauma on an individual.
- Detail the processes used in a "Critical Incident Stress Debriefing."
- Provide a guide for those who need to conduct Critical Incident Stress Debriefings.

Summary: Addressing the stress and trauma of NGO workers in insecure environments needs to be integrated into NGO security procedures. It is not unusual for individuals who have been exposed to a security situation to experience many of the symptoms associated with trauma and victimization. The physical and emotional aftermath can be very intense. This module details the skills and procedures used to address critical incident stress.

20. Security Information Management

Goal: To articulate the importance of maintaining a discipline of systematic reporting, analysis and communication of security related information.

Objectives:

- Identify the essential components of an incident report and a process for reporting.
- Articulate factors to consider in the analysis of an incident.
- Articulate a process/policy for communication/sharing of security related information both internally and externally.
- Articulate a process whereby evaluation of security information feeds into security planning.

Summary: Incident reporting is the basic element in security information management, and should also include the reporting of incidents averted. Further analysis of incidents should be done and fed into ongoing threat assessment and revision of security plans. Security information may be sensitive and mechanisms for communicating discretely must be considered. Incidents which happen to one agency may have implications for others. Therefore ways of sharing information which balance discreteness and transparency must be found.

Evaluation

For the courses, there were both formal and informal methods of evaluation, including the following:

- Daily written evaluations;
- Daily meetings with rotating representatives of the participants;
- Final written course evaluation;
- Final small group discussions, feedback, and plenary discussions;
- Solicitation of post-course feedback from participants returning to field (with a focus on the general usefulness of the course and use of course material).

Formal Evaluation Results

The formal evaluations provided to course participants resulted in the following conclusions:

- *Participants' objectives met*. Eighty percent (80%) of the responding participants indicated that the course met their objectives.
- *Experienced participants the most satisfied*. Participants with more than eighteen months of experience were more satisfied than those with less than eighteen months of experience.
- *Good exchange of ideas*. For both courses, 100% of the responding participants indicated that the course provided an opportunity to exchange ideas with others of similar interests.
- *Importance of different perspectives*. In the first pilot course, 100% of the responding participants indicated that the multi-agency and multi-national aspect of the course was essential.

> "Nationality affects how we perceive. How we perceive, or are perceived affects our security. Multi-national participation brought vivid examples of how perception can differ into the classroom." Toby Porter, OXFAM UK

- *Importance of regional training*. Participants indicated the course should be replicated regionally.
- *Importance of train-the-trainers*. In the first pilot course, which included a train-the-trainers (TOT) component, 96% of the responding participants indicated that the TOT component was essential. Many felt, however, that it would be helpful to lengthen the course, separating out the TOT component. As directed by USAID/OFDA, the second pilot course had no TOT component.
- *Mixed satisfaction with the weighting of topics*. Only 55% of the responding participants were satisfied with the weighting of the topics, though there was no clear consensus-by field/headquarters or amount of experience-on which ones

should be emphasized more and which less. Some found a need for greater focus on the conceptual aspects and others for greater focus on the technical.

"I returned from the security training on Monday evening and on Tuesday the US and British governments asked all of their citizens to leave Monrovia. Since the US embassy was under threat they could provide no assistance… The geography of Monrovia is similar to Flamingor City. This quick opportunity to put the security training to use enabled me to really assess what I got out of the training. More than anything else it was the development of a confidence to address a variety of security situations. I felt very sure of myself in knowing what factors to take into account in making decisions…So thanks for a very effective and relevant training." Sue Dwyer, International Rescue Committee

Working Group Observations

After developing the course modules and running two pilot courses, the Working Group agreed on several observations about the course that may be relevant to those considering future efforts in NGO security training.

Importance of Targeting Participants

While this course targeted personnel managing field security, the diversity among participants in the courses contributed both to the level of satisfaction and the level of frustration. It appears appropriate that there could be benefits from having three general types of security courses.

- *Basic personal security.* While not losing sight of the importance of relationships, analytical skills, and decision making, there is a clear need for a basic course in security for inexperienced field workers without security oversight responsibilities. Such a course could draw on the philosophy of the courses developed for this project and include the emphasis on interpersonal skills, but would focus relatively more on operational procedures and equipment, including vehicles and movement, site security, and telecommunications.
- *NGO security management*. This "level," the focus of the InterAction course, was determined to be the priority need by the NGO members of the Task Force, and the area with the greatest potential for impacting NGO security. To the extent participants in this type of course already have basic skills, the course could focus relatively more on analytical skills, decision-making, planning, and coordination.
- *Headquarters security awareness*. In developing and piloting the two courses, it became clear that there was a compelling need for a "knowledgeable commitment" from headquarters for field staff to achieve broad and effective implementation of improved security. To ensure that such a commitment exists, it would be important to have a short seminar/workshop on security to sensitize headquarters staff to the challenges of field security in new operating environments; identify and address points of conflict between headquarters and

field staffs; determine the headquarters-level policy implications of security issues; and address headquarters-level concerns such as liability issues and hostage negotiation.

Challenge of Training Trainers

To maximize security training it is important to train trainers, however this proved too much material to put into a one-week course. It was attempted in the first pilot with inclusion of a TOT component, which was eliminated in the second pilot. In both pilot courses, participants felt that there was not adequate time to cover everything they wished in the depth they wished. Future courses should be longer than one week to include a train-the-trainers component.

Materials Development

There is sill significant work to be done before a complete, refined NGO security management course is produced. As noted previously, during the development of the course it became clear that the traditional approach to security was not completely applicable to the NGO community. The Working Group, therefore, had to develop many of the modules with little to draw upon.

The result was a series of written products-modules and lesson plans-that remain in need of testing and refinement, and which do not cover every important issue. Although satisfaction with the course was very high, the Working Group concluded that further work is needed to make it more usable. To refine the material, the following efforts are required:

- Conduct research and develop materials on issues not yet covered in modules produced for the course, such as cash management and security coordination.
- Refine the contents of modules that address previously undocumented issues. For the security strategies module, for example, it is important to identify which security strategies have proven effective in different types of situations, as well as how to balance security strategies when faced with multiple types of threats.
- Field-test the materials developed.

To make the material more usable, following further research and field testing, it will be possible to further develop and refine the course design and exercises; synthesize the material in the form of a field guide; and develop a trainer's manual to accompany the field guide.

Regional, Research-Oriented Training

The need for more research and better documentation suggests that future work in this area might benefit from conducting integrated training and research which brings out the experiences of participants, and helps to identify good practices. Doing so on a regional basis would:

- Train more NGO personnel and obtain more feed-back;
- Field-test the material by interviewing those implementing it after the course;
- Facilitate research on issues such as region-specific security problems and solutions, interagency communication and collaboration on security, and national staff perspectives.

Contributors to the Course

Developing the course required the efforts of many people. We would first like to thank the following individuals and institutions who contributed to the work of this project by attending advisory Task Force meetings or by providing supporting documents: Jannie Armstrong of American Refugee Committee, Pete Bradford of OFDA, Lucy Brown of American Red Cross, Dave Brubaker, Christian Captier of Action Contre la Faim, Millie Casperson of American Refugee Committee, Frank Catania of Save the Children US, Kryss Chupp of Christian Peacemaking Team, Aline Curran of UNICEF, Philippe Dind of the International Committee of the Red Cross, Jonathan Dworken of the Center for Naval Analyses, Pierre Gallien of Action Contre la Faim, Harlan Hale of CARE, Andy Harris of ANSER, Pete Henderson of OFDA, David Jennings, Bob Kierce, Bob MacPherson of CARE, Randy Martin of International Rescue Committee, Gerald Martone of International Rescue Committee, Dawn McRae-Lopez of International Medical Corps, Tim Pasquarelli, Chuck Rogers of World Vision, Carolyn Shrock-Shenk of Mennonite Central Committee, Barbara Smith of International Rescue Committee, and Stephen Tomlin of International Medical Corps.

We would also like to thank members of the Security Working Group who developed the course modules and held the pilot courses.

- Jane Swan: jane_swan@hotmail.com
- Santhe Loizos: santhel@hotmail.com
- Lucy Brown: American Red Cross, 2025 E St. NW, Washington DC 20006, (202)728-6644, brownlu@usa.redcross.org
- Jan Davis: Red R, training@redr.demon.co.uk
- Jonathan Dworken: Center for Naval Analyses, 4401 Ford Ave., Alexandria VA 22302, (703)824-2637, dworkenj@cna.org, jdworken@hotmail.com
- Dave Dyck: dyckd@emu.edu
- Rob Lowe: Cable and Wireless Unit, 1375 Aztec West Business Park, Bristol, BS12 4RY UK, Rob.Lowe@plc.cwplc.com
- Michael O'Neill: Peace Corps, 1111 20th St. NW, Washington DC 20526, (202)692-1470 moneill@peacecorps.gov
- Lisa Schirch: Eastern Mennonite University, Conflict Transformation Program, 1200 Park Rd., Harrisonburg VA 22802, (540)432-4497, schirchl@emu.edu
- Koenraad Van Brabant: Overseas Development Institute, Portland House, Stag Place, London SW1E 5DP UK, k.brabant@odi.org.uk

This group intends to continue to work together after the closing of the project at InterAction. They may be contacted through the Project Director or individually.

Authorship of specific modules is noted on each module in the course binder, which is available through InterAction.