



Reflecting on Risk and Security Management

A learning case based on the experience
of the Berghof Foundation for Conflict
Studies in Sri Lanka

Summary

This learning case paper reflects the experience of the Berghof Foundation for Conflict Studies in Sri Lanka in establishing adequate risk and security management. It aims to share how we coped with a deteriorating security situation and outlines the adopted measures and activities. The core part of the document is the presentation of

ten essential elements of Berghof's risk and security management. Remaining dilemmas and controversial issues are also highlighted and we complete this learning paper with reflections on the strengths and challenges of our security performance.

Contents

The Berghof Foundation for Conflict Studies in Sri Lanka.....	3
1. Introduction and background	4
2. The changing situation for NGOs in Sri Lanka: threats and serious security incidents	5
3. What are the causes for the risk Berghof faced in Sri Lanka?	6
4. The ten elements of Berghof's risk and security management.....	7
4.1. Security training – a kick off point for following activities	8
4.2 Security plan – defining the security strategy	9
4.3 Security committee – focal group and driving force	10
4.4 Awareness building – lively discussions are welcome	11
4.5 Risk analysis – not a clear and logical science	12
4.6 Communication and media strategy – proactive communication	13
4.7 Internal communication – the ability to make a quick response	15
4.8 Coordination with other organisations – a challenge for conflict transformation organisations	16
4.9 Building a security net – diverse ways to strengthen relations	17
4.10 Security company – part of a deterrence strategy	18
5. Dilemmas and controversial issues	19
6. Reviewing strengths and challenges: what was successful and what needs to be improved?.....	21
7. Bibliography	22

Imprint

© Berghof Foundation for Peace Support 2008

Print versions of the complete study can be ordered at Berghof Foundation for Peace Support
Altensteinstr. 48a, 14195 Berlin, Germany
Phone +49 (0)30-844.154.0
home@berghof-peacesupport.org

Text Author: Gregor Maaß
Contact: Barbara Unger
Graphic and illustration design: COXORANGE Grafikdesign
Illustration master: Lucie Noll
Printed by: schöne drucksachen

The Berghof Foundation for Peace Support would like to acknowledge the support received from the German Federal Ministry of Economic Cooperation and Development (BMZ) through the Deutsche Gesellschaft für Technische Zusammenarbeit (GTZ) GmbH and the Swiss Federal Department of Foreign Affairs (FDFA).

The Berghof Foundation for Conflict Studies in Sri Lanka

The Berghof Foundation for Conflict Studies in Sri Lanka was established in 2001 on invitation of the Sri Lankan Government, based on a Memorandum of Understanding with the Ministry of Constitutional Affairs. It was jointly funded by the Swiss Federal Department for Foreign Affairs (FDFA, PDIV) and the German Federal Ministry for Economic Cooperation and Development (BMZ) through the German Technical Cooperation agency (GTZ). Its mandate was to enhance and support the capacities for constructive conflict transformation in Sri Lanka and to implement the Resource Network for Conflict Studies and Transformation (RNCST). The work of the Berghof Foundation in Sri Lanka ended as planned at the end of 2008, after a predefined period of 8 years, while its office closed already in mid 2008. The Berghof Foundation for Peace Support (BPS), based in Berlin, was responsible for implementing the Sri Lanka Project.

Mission Statement

Support the peace process in Sri Lanka at the track 1 and 2 levels, in collaboration with Sri Lankan partner organisations, by providing capacity building, reviewing, dialoguing and problem-solving opportunities for all principal stakeholders.

Principles

Multipartiality: As an independent conflict transformation organisation, one of the key challenges faced by the Berghof Foundation in Sri Lanka from its inception has been the maintenance of a good working relationship with all stakeholders in conflict and peace. Achieving this balance, while at the same time maintaining independence and professionalism, has often been difficult. However, patience, time and an appreciation of the Berghof approach – which hinges on empathy with the needs and fears of all parties – convinced many (though, unfortunately, not all) stakeholders of the merits of multipartiality as a key principle of our engagement in Sri Lanka.

Domestic ownership: We believe that the final resolution of the Sri Lankan conflict has to be one developed and agreed by Sri Lankans themselves. Therefore we did not advocate any particular solution to the conflict in

Sri Lanka. Rather, we were committed to helping Sri Lankan stakeholders find lasting peace for all communities in Sri Lanka.

Confidentiality: Once basic trust and confidence had been established, we brought various parties, groups and constituencies together in one room, to discuss common issues and the problems arising from them and to explore possible solutions to these problems. While some such engagements were open, others were restricted in terms of participation because the issues discussed were sensitive and of particular importance to the parties in question.

Critical interaction: We adhere to international humanitarian and human rights law and do not approve of any kind of violence. We also condemn undemocratic rule and violations of the rule of law, but we are not an advocacy organisation and do not publicly condemn any activities of the parties to the conflict. Nevertheless, we made our stance and our constructive criticism well understood through dialogue and direct interaction. As a conflict transformation organisation, our role is to help the parties emerge from cycles of violence through constructive engagement.

Four core functions

Capacity building: We helped to build capacities of persons, institutions and networks engaged in peace building, providing them with access to information, external expertise and opportunities to travel abroad in order to learn from similar experiences of practitioners and academics from different parts of the world.

Dialogue: We encouraged and facilitated dialogue, contacts and communication between the members of the parties in conflict.

Track 1.5 engagement: We offered advice and maintained a critical-constructive engagement with relevant stakeholders from all conflict parties, especially on track 1.5.

Financial support: We provided financial support to partner organisations and their programmes.

1. Introduction and background

When the Berghof Foundation for Conflict Studies started to implement the Resource Network for Conflict Studies and Transformation (RNCST) in Sri Lanka in July 2001, we hardly anticipated that setting up proper risk and security management would be a crucial task within our organisation. We were enthusiastic about providing support, assistance, external experiences and knowledge to local stakeholders, but reflecting on our security performance was in fact a minor issue. As a result of the deteriorating security situation for Berghof and also for other organisations in Sri Lanka, we were required to improve in this field up to the integration of internal security and risk management.

Due to changing political dynamics our Berghof team, based in the capital Colombo¹, had to face several security incidents, in particular a number of attacks in critical and offensive newspaper articles, primarily appearing on the internet, in Sinhalese language daily newspapers and in the newspapers of certain political parties. Analysing these incidents we became aware that the risk we were facing as an organisation was directly related to our core work. We started gathering experience in the field of security through training sessions and internal discussions and we learned an important lesson: risk is a factor we can work with and we can cope with. Since then, Berghof has adapted different measures and activities to face the deteriorating security situation.

As a consequence of the attacks and criticism, our work suffered an abrupt change when the residence visa for our director was unexpectedly revoked in January 2008. In consultation with our donors, and after numerous communications with our partner ministry, we took the decision to cancel the Memorandum of Understanding with the partner ministry because our basic requirement for carrying out activities in Sri Lanka was no longer guaranteed. We closed our project office at the end of July 2008 and most activities were also concluded at that time. The whole project was wound down as planned at the end of 2008, after the predefined period of 8 years.

By compiling this learning case paper we want to share our experience with our partner organisations in Sri Lanka, practitioners in the field of conflict transformation, organisations working on conflict, donor organisations and any other interested people. Along with the available security manuals, we hope that the lessons learned within this document can be useful to others. Additionally we will highlight some dilemmas and controversial issues that demonstrate the complexity of the subject and reveal that security performance is never a finished work, but always a work in progress.

The aim of this learning case paper

- Sharing Berghof's experience of how we learned to cope with a deteriorating security situation and how we established our risk and security management.
- Outlining security measures and activities adopted by Berghof in Sri Lanka.
- Highlighting controversial issues and dilemmas regarding our security performance.

2. The changing situation for NGOs in Sri Lanka: threats and serious security incidents

The Sri Lankan conflict has been described as a paradigmatic case of protracted social conflict, where the main warring parties are the non-state armed group Liberation Tigers of Tamil Eelam (LTTE) and the Sri Lankan Security Forces. The conflict has developed over a long time through the interaction of many factors: the centralisation of power and administration, majoritarian politics and structures, relative deprivation of communities in the Northeast and the South, the militarization of political movements and the tragic cycles of violence and counter-violence, of terrorist attacks, of political assassinations, of gross human rights violations and mass displacement of people.

Against this background, there are a number of local and international non-governmental organisations (NGOs and INGOs) involved in the process of developing a lasting peace in Sri Lanka and providing development aid in the affected regions. These organisations are working in an increasingly hostile environment and many of them have suffered serious security incidents.

Where do the hostile attitudes towards NGOs come from? NGOs are often perceived as an intervention into the sovereignty of Sri Lanka. As this sovereignty is in dispute by the warring parties, any intervention by NGOs is seen as suspicious. The main accusation against NGOs (especially INGOs, but also against donor organisations and even the United Nations) is that they allegedly support the LTTE, even if their purpose is explicitly neutral. This misinterpretation of NGOs' mandates is alarming and it affects the important contributions that NGOs can make to peace, welfare and justice.

Apart from these accusations, INGOs working in Sri Lanka are faced with a particularly strong rejection of international involvement in national issues. This is grounded in the historical roots of the anti-colonial struggle and has been instrumentalised by national hardliners. After the tsunami in December 2004 the situation deteriorated even more, as the government voiced strong criticism against international relief agencies and accused them of not fulfilling promises

but using aid money supposedly for personal indulgence and political gain. A turning point for INGOs' security was the change to a new government in April 2004, supported by and partially composed of nationalists with a critical and aggressive INGO discourse.

The consequence of the hostile environment for NGOs in Sri Lanka is the existence of a wide range of threats. The most noticeable threat to NGOs is the aggressive media coverage, in print media and television. Nationalist lobby groups with great influence on the press

Aggression experienced against NGOs working in Sri Lanka

- Hostile and defamatory statements in the media (press articles and television).
- Stage protests arranged by lobby groups carrying out violent actions.
- Disruption of programmes due to organised protests and aggressions.
- Raids of NGO-office premises.
- Abduction and killing of national staff and expulsion of international staff.

maintain constant censure against NGOs in public, and hostile articles are frequently published. It is also common that organised stage protests are arranged by lobby groups in order to voice criticism against NGOs, verbally or even violently. In particular cases these organised protests have resulted in office raids, presenting a significant risk for the affected organisations.

While threats to conflict transformation organisations were conveyed in subtle forms like defamation and false accusations, INGOs engaged in development aid were subjected to obstacles such as delays in issuing work permits or travel restrictions, and they have also been physically attacked. During 2006 and 2007 we had to observe an escalated level of tragic abduction and killing of local staff from several development organisations, such as the Red Cross, Action Contre La Faim and the Norwegian Refugee Council. In 2008 the situation became increasingly difficult for international organisations and even personnel from the United Nations were refused their resident visas.

As these above-mentioned risks are not far-fetched but a reality in Sri Lanka, we learned that we needed to take steps to prevent such situations and that we would also need to be prepared in case they did occur.

3. What are the causes for the risk Berghof faced in Sri Lanka?

Analysing the relation between the risk and our work, we have to consider that in part we were faced with the same threats as other NGOs and INGOs. In this sense, Berghof was also affected by the hostile attitude and the rejection of international involvement. Berghof was also threatened by negative press coverage, receiving its first series of press attacks after the elections and the change of government in 2004. Several newspaper articles started to appear in 2006, after the transmission of a popular TV-programme in which Berghof was discredited with false information. Furthermore Berghof suffered the disruption of a workshop on “Constitution-making” in South Colombo in 2006, caused by spontaneous protests following an LTTE attack not far from the workshop venue.

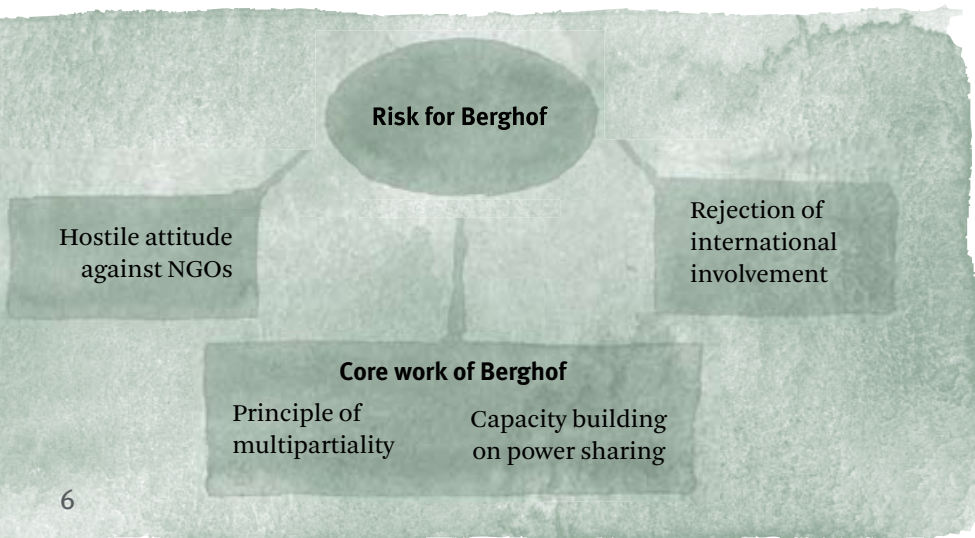
As an organisation working in the field of conflict transformation and using innovative working principles, we additionally had to cope with particular risks. Here we want to remark on two risks with regard to our core work, firstly our principle of multipartiality and secondly our engagement in capacity building on sensitive issues such as federalism and power sharing.

Berghof’s multipartial approach for conflict transformation favoured constructive engagement with all stakeholders to achieve a negotiated solution to the armed conflict. This means empathising with the basic needs and concerns of all communities and principal parties to the conflict and impressing on them the importance of including all of them in a fair and just

process of conflict transformation. The former peace process, established during the government period of the United National Party (2001-2004), and the cease-fire agreement from February 2002 made it possible to apply this multipartial approach. During this time Berghof was able to develop dialogue processes with southern and northern stakeholders, including the LTTE. Yet when the peace process started to fail from 2003 on, and when the government of Sri Lanka changed into a coalition of the Sri Lankan Freedom Party (SLFP) and Janatha Vimukthi Peramuna (JVP) in April 2004, Berghof was criticized and attacked by influential nationalist groups for its dialogue processes with the LTTE and for having been close to the former government party UNP, which was now in opposition. This dynamic meant that multipartiality as a core working principle of Berghof caused us a significant risk that we had to cope with.

Our engagement in capacity building on federalism and power sharing is a sensitive and controversial issue in Sri Lanka and was closely related to the risks we faced as an organisation. During the peace talks the conflict parties agreed in the so called Oslo formula to “explore” federalism, and subsequently the government of Sri Lanka requested Berghof to carry out capacity building in this area. Hardliner nationalists rejected the option of power sharing as a solution for the conflict, and when they became part of the new government after the elections in 2004 they opposed Berghof’s programme and attacked the organisation. The

reasons behind this are multiple and a major issue is also the struggle for power, where the new government wanted to lay blame on the former one which had invited Berghof to support the peace process. This situation exposed us to a significant risk.



4. The ten elements of Berghof's risk and security management

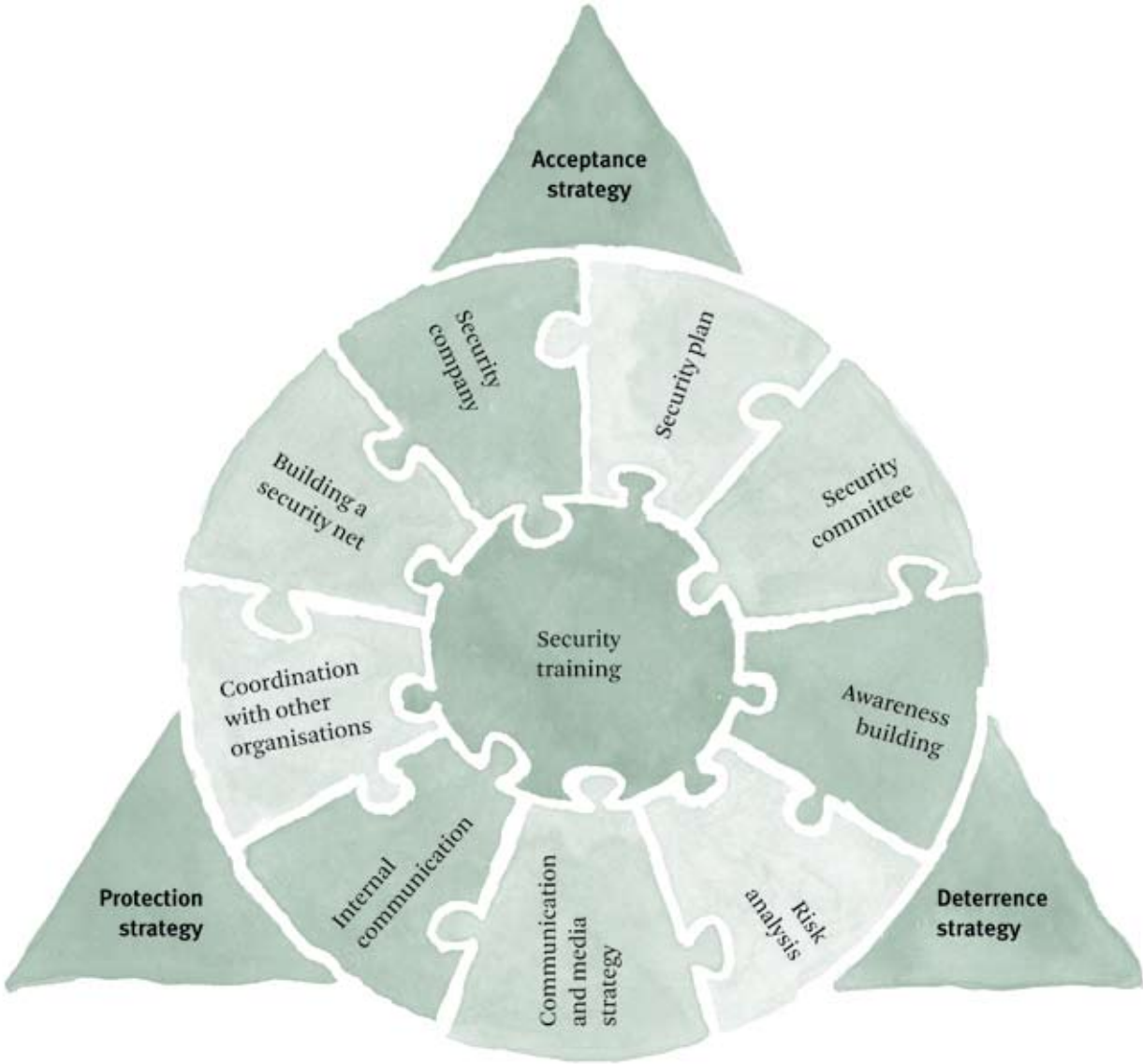


Diagramme: Berghof's risk and security management

The following points describe the ten essential elements of Berghof's risk and security management in Sri Lanka. On one hand these elements reflect what we have learned through training and from existing security manuals. On the other hand, and certainly more interesting for the reader, these elements have a close practical relevance, since our security performance emerged out of a concrete need and is based on our experience.

While our initial responses to most security incidents were rather incomplete and tended to be personalised with action taken just at an individual level, in the course of time we improved in knowledge, analysis, reaction and action. Within these ten points we want to get our experiences across, highlighting some aspects of special interest without omitting problems or difficulties.

4.1 Security training – a kick off point for following activities

The first security incidents affecting Berghof were aggressions by the media based on personal attacks, mainly against programme staff. At this time responses were just made on an individual level by the affected persons. Berghof supported the affected staff, but an organisational mechanism to safeguard against these attacks, to manage and respond to such incidents did not exist in its entirety. But when the aggressions intensified, the Berghof management felt the need to address security as an organisational issue. We sought the assistance of an external security expert to deliver security training and to bring security onto the agenda of our organisation in a proactive way.

There are different strategies regarding who should be trained. While some organisations decide to prioritise certain groups of staff or key groups, others follow a strategy of providing a basic level of security training to all staff (ECHO 2004, p. 32). Berghof opted for a combination of both, and had two training sessions:

1. The first session was addressed to the whole Berghof team in Sri Lanka, including drivers and office support staff. The objective of this part was to share experience on concepts of security management, and to improve the skills to make a global assessment of the security policy of Berghof in Sri Lanka. Part of the proceeding was to assess all possible threats to Berghof, which helped us to understand the risks involved.
2. The second session was aimed at a limited number of key staff, selected to drive the initial process in order to hand over to a security committee later on. The session aimed to improve the necessary skills for introducing institutional changes in order to improve both the policy and the implementation of security in the organisation.

In retrospect this training was very useful and served as a kick off point for many other activities which followed. The participation of the whole team helped us to make risk and security an issue of discussion among Berghof staff and was useful for raising awareness. From the evaluation of the training we learned that it is advisable to include practical and operational guidance into the training programme. For example, an initial training session should include a review of the concrete threats and it should help to formulate strategies on how to handle situations of threat, because this is what affected persons are most interested in. Hence when designing such training we would recommend including a theoretical part, giving a holistic understanding of security, and also a more “hands on” part.

The choice of the trainer is important, as it already indicates how we want to cope with security risks. Trainers usually focus the sessions according to their backgrounds and while some will emphasize protective or deterrent measures, others will treat security with a more holistic approach. Berghof chose the latter and worked with a trainer who has a background of working with human rights defenders. This choice was adequate, since Berghof required measures that go beyond protection and deterrence.

Following the initial security training, selected Berghof staff took part in additional training sessions on special issues such as security management and driver training. Continuing training activities were welcomed as a way of getting new input on security measures and they also helped to keep discussions on security alive within the team.

Key lessons learned

- Security training should target both the wider team, with full participation of staff, and a smaller group with key staff selected to drive the initial process, providing them with knowledge about how to introduce institutional changes.
- Initial security training sessions are best designed with a theoretical part and a more “hands on” part.
- Conflict transformation organisations should choose trainers who use a holistic approach to security.

4.2 Security plan – defining the security strategy

The security plan frames the general security approach of an organisation and defines the security strategies adopted in order to control the risks. Three ideal-type security strategies exist: acceptance, protection and deterrence (Van Brabant 2000, p. 57). The acceptance strategy tries to reduce or remove threats by increasing the acceptance for your work in a particular context. A protective strategy uses protective procedures to reduce the vulnerability of the organisation. The deterrence strategy attempts to deter a threat by making a counter-threat. In Koenraad Van Brabant's (ibid.) words: "Acceptance is about making more friends, protection about sheltering at a distance, and deterrence about intimidating your enemies." Berghof decided to adopt a combination of these strategies, with most of its measures taken to create more acceptance and only limited activities oriented towards a deterrence strategy.

The security plan also defines responsibilities and decision-making structures for emergency situations and gives instructions for action in situations that are likely to happen – the so called Standard Operating Procedures (SOPs). For example, after a few cases of office raids targeting international organisations in Colombo, this risk also became real for Berghof and we worked out what we would have to do in the case of an office raid and how we could be best prepared for such a threat.

In this sense the security plan cannot simply adopt SOPs from other contexts but needs to respond to the real risks the organisation is facing. It is also important that these SOPs are well practiced, e.g. in the form of role-plays.

What we have learned is that for making the security plan a useful document, the process of compiling it is just as important as the plan itself (VENRO 2003, p. 11). In our case it was the task of the security committee to elaborate the security plan in consultation with all staff members. We think that it is important that the team participates during the compilation process to make the plan appropriate to the given situation, to consider valuable information and insights especially from local staff and to secure ownership for the plan. Only if the whole team is involved in compiling the plan can we expect that everybody will comply with it.

The security plan needs to be understood as just one element of risk and security management, and if we want it to be a useful document we need to work with it: some sections need regular updating, the instructions for action in emergency situations need to be practised in simulations and the lessons learned from security incidents need to be integrated systematically.

Central chapters of Berghof's security plan

- Statements on the objective, the compilation process, the responsible persons, implementation and updating
- Guiding principles for security defining the security strategy of the organisation
- Background information of the organisation (mandate, principles) and on the context of the operations to provide staff with an overview to better understand the subsequent instructions for action
- Standard Operating Procedures (SOPs) that refer to recurrent events or to predefined emergency situations
- Contact details for emergencies

4.3 Security committee – focal group and driving force

One of the main recommendations from the initial training was to set up a security committee so that the organisation would be able to continue working on the topic in a more institutionalised way. This committee was commissioned to act as a focal group and driving force for all security related issues.

Finding the best solution for a security management structure might differ in relation to the size and type of the organisation. Ideal-type models are: a) the management-line model where responsibility lies only with the operational management, b) the specialist security officer model where one or more specialists are located in the field and c) the security advisor model, which combines the two models above and where the responsibility for security lies with the operational management but a security focal point provides specialist back-up (Van Brabant 2001, p. 19).

Key lessons learned

- It is advisable to secure participation from all areas of the organisation for the security committee and to include management staff to ensure an adequate overall perspective.
- The necessary resources and time need to be allocated to ensure long-term engagement of the security committee.

Berghof, with a team of about 20 staff members, fared well with a security committee composed of four persons from different areas of the organisation. We have learned that broad participation from all areas of the organisation (administration and programmes) is important for functioning effectively, because security is a crosscutting issue that affects all aspects of the organisation.

At first, Berghof opted for a model that excluded management staff from the security committee for reasons of their limited availability and the possible amount of time they could dedicate to the committee. Since then

we have come to recognize that management staff should be a part of the security committee because security requires an adequate overall perspective, which cannot be guaranteed fully without the participation of management staff.

For the composition of the security committee it is also important to consider other criteria such as trustworthiness, confidentiality, gender balance, availability and also training skills, as the committee might consider it necessary to further train the team members. Regarding the security committee's tasks, in the short term the committee (in consultation with all staff) developed a security plan, taking into consideration the existing risks and threats posed to the organisation. In the long term the committee had the function of ensuring the implementation and management of the security plan, with appropriate action taken in instances of

emergency and other reported security incidents. Another important task of the security committee was building awareness for risk and security within the team and also being a contact point for confidential conversations about security incidents.

It was not easy to maintain long-term engagement of the security committee. Especially at times when the risk is apparently low, the dedication of this group will also decline because other topics become more important within the organisation. This is acceptable as long as the organisation fulfils basic requirements such as updating the risk analysis, and the security committee stays alert so as to get involved when required. Here it is important that the organisation allocates the necessary resources for the committee to function adequately. Staff involved in the committee should have the time available for meetings and updating documents, and the time dedicated to the security committee needs to be marked in the work plan.

4.4 Awareness building – lively discussions are welcome

Living in a violent context such as in Sri Lanka's capital Colombo and always being exposed to a certain level of risk, everyone makes personal security considerations every day. The perceptions of risk vary greatly as they depend on the person's individual background and previous security experiences. Risk awareness among Berghof staff members had to be raised, in order to accept the different communities' and individuals' perceptions, fears and vulnerabilities.

Initially it was difficult for Berghof staff to think beyond their own personal security towards more organisational security, but in fact working at Berghof in Sri Lanka exposed every single staff member to another risk, a more organisational risk. The team learned to understand that we faced an inherent risk that was related to the character of Berghof's work of conflict transformation and that having appropriate security management was precisely what enabled us to carry out this work.

Working on conflict may also lead us to think that risks are part of the work and that there is no need to speak about it, or we might not allow ourselves to acknowledge our fears. Therefore it is fundamental to


exchange perceptions of risk within the team, reflecting on our own willingness to take a certain risk and create an analytical understanding of the risk our organisation faces because of its work.

Building awareness is crucial for organisations because "effective security management ultimately relies not on documents but on skill, discipline, alertness and information exchange. [...] Security and risk control must be routinely and explicitly on the agenda in interactions and discussions and at key moments in the professional assignment cycle of the aid worker." (Van Brabant 2000, p. 320)

The initial security training contributed to creating risk awareness in Berghof and the team members became more sensitised to security discussions. Furthermore the security committee developed a series of activities to maintain alertness and to keep alive the reflections on risk and security within the Berghof team. Emergency simulations such as office raids realized in the form of role-plays were greatly welcomed, but the frequency of such simulations should not overstrain the team.

Key lessons learned

- Risk awareness needs to be raised in order to accept the different communities' and individuals' perceptions, fears and vulnerabilities.
- Working on conflict transformation implies reflecting on our own willingness to take a certain risk.
- Activities such as security training and emergency simulations contribute to creating risk awareness.



Awareness
building

4.5 Risk analysis – not a clear and logical science

In theoretical terms there is a broad standard of knowledge about risk. According to this, risk refers to possible events, however uncertain, that result in harm (Eguren and Caraj 2008, p. 27). Risk can be seen as a function of the threat against us and our vulnerabilities, which can be compensated by capacities (ibid. p. 28):

$$\text{Risk} = \frac{\text{Threat} \times \text{Vulnerability}}{\text{Capacity}}$$

This formula gives a plausible understanding of risks but it is not applicable in a simple way because risk analysis is not a clear and logical science. Analysing our risks means finding a reasonable understanding of the relationship between threats, security incidents, vulnerabilities and capacities, the political situation and the work of Berghof both in general and in particular at the current moment. Here theory additionally suggests that for assessing our risks we need to analyse the main stakeholders' interests and strategies and the impact of our work on those interests and strategies. By knowing more about this relationship and analysing our threats, vulnerabilities and capacities we can establish what kind of risk we are facing (ibid. p. 27).

Even though the theory offers good approaches, it is difficult to put them into practice. For Berghof in Sri Lanka the changing political environment, especially after the breakdown of the peace process and the change of government in 2004, implied a mayor shift with respect to our risk and we were slow in realizing this interrelation. We tended to behave more reactively than proactively, we did not update the conflict analysis frequently enough and did not think through all consequences of the changing situation.

What needs to be considered for improved risk and security management? Risk analysis should not only

be done retroactively after a security incident has happened; a proactive risk analysis is also necessary in order to anticipate risks, avoid them or be better prepared for them (Van Brabant 2000, p. 48). Thinking in terms of possible scenarios can help to analyse risks from a proactive perspective.

Our security committee was commissioned to establish and guide the risk analysis sessions, but the responsibility for good risk analysis lay within the whole team. It was a big advantage that individuals with very diverse personal backgrounds made up the Berghof team, because the diversity of information and insights were of considerable value in correctly assessing the situation. Each staff member had their own networks of information that contributed to a broad understanding of the situation. The joint team meetings and conflict analysis updates served as a good place to exchange on risk matters and security incidents, and a systematic analysis of this information helped forge a better understanding of the risks Berghof had to cope with.

The risk analysis should lead us to improve our security performance and it should help to conclude what changes we need to make regarding our work and activities and our security strategies. Theory suggests that a “basic feedback loop” should allow the risk analysis to feed into the working plan (for instance with conclusions to modify a workshop plan) and into the security plan (for instance to establish a new SOP for the case of violent workshop disruption). A “strategic feedback loop” goes up to the strategic stage, allowing the risk analysis to feed into the scenario analysis in the designing of the programme (Eguren 2000, p. 3). Conclusions from the risk assessment should also be integrated into simple routines, such as security checking locations as part of the preparation for seminars or assessing possible public relations options for each activity to make our work more transparent and more accepted.

Key lessons learned

- Even if theory offers good approaches, in practice it is difficult to establish systematic and permanent risk analysis.
- Proactive risk analysis and thinking through the consequences of possible and real changes in the political environment is crucial.
- The whole team should be involved in the risk analysis, to enrich it with diverse personal insights and information networks.
- The conclusions from the risk analysis must be integrated into simple routines and they need to feed into the security plan, the work plan and into the organisation's strategy.

4.6 Communication and media strategy – proactive communication

Making a new communication and media strategy part of our risk and security management resulted from a direct need, because the most visible threats were the attacks through the media, especially in the print media but also on television. A series of articles were released containing defamatory statements and disseminating false information, in particular in the vernacular press.

Over the first four years in Sri Lanka Berghof maintained a rather low profile within the media. This was the preferred option because of the sensitive nature of the dialogue promotion work requested from all stakeholders in the conflict. With the shift in the political environment, opponents to our work started to make use of their strong media connections and initiated a destructive press campaign. As we had never engaged the media in a structured way, there was only limited knowledge about the organisation in public and in the media. Consequently hostile articles, primarily appearing on the internet, in Sinhalese language daily newspapers and in the newspapers of certain political parties, had a vast negative effect.

Berghof's first response to the critical articles was to write back a public statement to the newspaper that was then again answered and soon we realized that we had got engaged in an unproductive back-and-forth of articles and responses. We learned that we would have to become proactive in a smarter way.

In 2006 Berghof shifted its communications and media strategy from a low profile approach to a more proactive strategy. The communication unit was reorganised and we focused on a change of mindset and attitudes within the whole organisation. The implementation of the new strategy was difficult, because trying to make up for what we had not done over the first five years was a challenging task.

Realizing that our working habits had meant that we were not as transparent about our work as we would like to be, we started to disseminate press releases for activities like workshops. Here we needed to strengthen the internal communication between the programme and the communication unit to make the academic styled information understandable for a wider public.

Communication
and media
strategy

Key lessons learned

Communicating our work in a transparent and proactive way contributes to creating acceptance for it, while a low profile within the media can be counterproductive.

Some important elements of an appropriate communication and media strategy:

- Disseminating press releases for activities (also in local languages)
- Inviting the media to understand our work
- Giving answers to key questions and allegations raised by our critics through an FAQ section on the website

As most critical articles were released in the vernacular press, we also started to translate press releases into the local languages Sinhalese and Tamil.

Another element of the new communication and media strategy was to be proactive and transparent by inviting journalists and newspaper editors to familiarise themselves with our work and with issues of conflict transformation in general. Also we carried out activities like training specifically catering to journalists, to create linkages and understanding and to further support them in their work.

We also renewed and improved our website, Berghof's "public face", and added a Frequently Asked Questions (FAQ) section. The extensive FAQ section gave responses to some of the key questions and allegations raised by our critics. It contributed to more transparency and furthermore was extremely useful for our staff because then everybody had clear guidelines for how to respond to partner organisations and friends concerned about the accusations in the hostile press articles.

Another issue contributing to more transparency was that Berghof was summoned before the Parliamentary Select Committee for the Investigation of the Operations of NGOs (PSC). Since we were not accredited as an INGO in Sri Lanka and due to our status of carrying out official development cooperation between the governments of Sri Lanka, Germany and Switzerland we were unclear as to how to respond to this summons. Eventually, after receiving clarification from the German and the Swiss embassies as well as other Sri Lankan partners, we appeared before the PSC in two constructive and successful sessions. As other organisations had previously found that the PSC declarations had triggered a hostile media trial, it was important for us to have a clarifying conversation with the PSC and to respond to every doubt and concern.

The adapted communications and media strategy is one of the most important elements of our risk and security management. Communicating our work in a transparent and proactive way has contributed to creating acceptance for it.

4.7 Internal communication – the ability to make a quick response

When Berghof experienced the disruption of a workshop in Colombo in 2006, the team learned that the internal communication within Berghof needed to be improved and adapted to situations of emergency that could require rapid decision-making. In this specific case, while a crowd of protesters was gathering outside the venue, the Berghof workshop team had to consider an appropriate reaction in the absence of the senior management staff who were usually in charge of taking decisions.

For such moments it is crucial to have pre-clarified decision-making structures and a well thought out internal communication structure. In fact an organisation can never be perfectly prepared for everything that might happen and therefore it is essential to be able to communicate and to react rapidly the moment a security incident occurs.

Following on from the workshop disruption, Berghof developed clear guidelines about who was responsible for making decisions and who needed to be consulted for making decisions. Special security procedures were

introduced for recurrent situations such as the realisation of workshops, which included checking the venue before the event and nominating a person in charge for decision-making.

Furthermore Berghof introduced an internal telephone cascade for rapid communication within the team. In case of emergency every staff member should be contacted directly to receive warnings or other important messages. Everyone knows their position in the cascade and will subsequently contact others in the cascade to pass on the message. This system therefore does not rely on individuals contacting and re-contacting a single person in charge but permits quick and flexible communication. The person on top of the cascade can be reached 24 hours a day and will be contacted first in case of emergency.

Apart from this internal cascade, some members of Berghof were part of other emergency networks and sms-trees. In doing so, Berghof had access to relevant security information and could pass it on to staff members.

Key lessons learned

- For rapid reaction in an emergency situation it is essential to establish pre-clarified decision-making and communication structures.
- Specific recurrent events such as holding workshops need specific pre-designed security procedures.
- A telephone cascade is a useful tool to ensure rapid communication within the team.



Internal communication

4.8 Coordination with other organisations – a challenge for conflict transformation organisations

Coordination and exchange on security with other organisations is important to share relevant information, to enrich our own risk analysis and at an advanced stage it allows sharing of risk by undertaking joint actions. Recognizing this, Berghof has made efforts to increase exchange with other organisations in Sri Lanka.

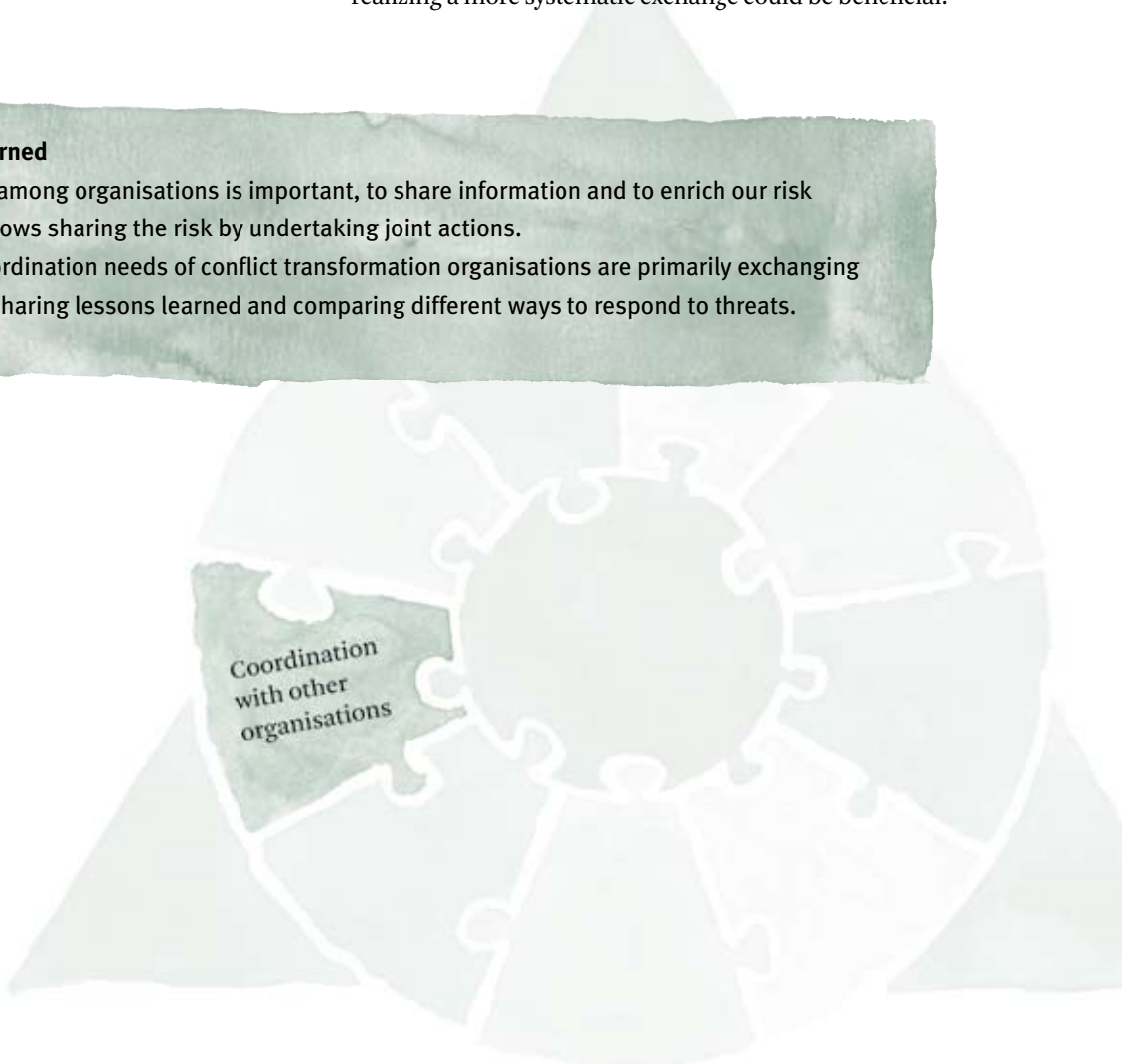
The challenges for security coordination among agencies and organisations are broadly reflected in security studies and include “the sensitivity of the information being shared, as well as the possibility of local sources being compromised and their confidentiality being breached. This makes agencies cautious in their approach to security coordination.” (Stoddard, Harmer and Haver 2006, p. 29)

Despite these types of challenges there is a considerable degree of security coordination in Sri Lanka, but mostly among humanitarian organisations. These existing forums are not appropriate for a conflict transformation organisation like Berghof, since the issues discussed are mostly focused on humanitarian aid in the field. Exchange within organisations engaged in conflict transformation has taken place only sporadically and only referred to specific threat situations, not to a joint security approach.

Initially the type of coordination needed by conflict transformation organisations in Sri Lanka does not necessarily mean formally “coordinating” security but rather establishing an informal exchange of information, sharing lessons learned and comparing different ways to respond to threats. Even though some exchange already exists, realizing a more systematic exchange could be beneficial.

Key lessons learned

- Coordination among organisations is important, to share information and to enrich our risk analysis. It allows sharing the risk by undertaking joint actions.
- The initial coordination needs of conflict transformation organisations are primarily exchanging information, sharing lessons learned and comparing different ways to respond to threats.



Coordination with other organisations

4.9 Building a security net – diverse ways to strengthen relations

In the light of increasing attacks, Berghof built up a security net by strengthening its relations to several actors. Continuous relations to external persons, organisations and institutions were very useful for receiving advice at a given moment, or for having the communication channels established in case it came to a point when we would need to make use of them. The following elements of a security net have proven to be useful for us:

One element is Berghof's net of friends. The idea behind this kind of net is that there can be mutual support between Berghof and friends in civil society, partners and stakeholders like ambassadors or leaders within multilateral organisations which serves as a safety net at critical times. Therefore Berghof made efforts to ensure continuous exchange and interaction with diverse friends, informing them of the current status of the organisation in terms of programmes and priorities. In practice it was difficult to "formalise" this net but very useful advice was given to us in certain situations. To avoid unfulfilled expectations it is important to have a realistic feeling of what the friends would be able to do in what kind of situation.

Another part of Berghof's security net is the relation to our donors, or rather their representation through the German and the Swiss embassies. Both embassies reacted very supportively when we were facing security problems. From our experience we think that conflict transformation organisations should consider introducing security as a topic of discussion with donors from programme inception on, to create awareness for the risk prone nature of their work. Informing donors systematically on the current security and risk situation, and updating them proactively about the most sensitive work, would help to maintain awareness for an organisation's security needs.

A third element of Berghof's security net is the establishment of good communications with the police station. To ensure a quick response we registered our staff members at the nearest police station and maintained contact with the officer in charge.

Key lessons learned

Building a security net through strengthened relations with several actors has proven to be useful.

Three elements of a security net:

- Establishing mutual support between Berghof and friends serving as a security net in critical times.
- Include security as a topic of discussion with donors to raise awareness for risk prone work.
- Registering at the police station to ensure quick communication.



4.10 Security company – part of a deterrence strategy

The use of security companies is a common but controversial part of an organisation's security performance, based on a strategy of deterrence. In contrast to the strategies of acceptance or protection, the deterrence strategy attempts to deter a threat by making a counter-threat. Additional current deterrence options are to threaten with sanctions or with the withdrawal of operations. Making use of security companies is a demonstration of power and control that affects the image and perception of an organisation, and it is of course even more problematic if the use of arms is considered.

Since the beginning of Berghof's programme in Sri Lanka a security company was employed to provide unarmed security guards for the entrance gate. In Sri Lanka it is very common for international organisations, bigger local NGOs and INGOs but also for companies and private residences to have security companies protecting the premises. Even for a conflict transformation organisation like Berghof, which would prefer to abstain from this kind of deterrent demonstration of

power, it was necessary to adapt to the reality of the country and to fulfil the common standards so that no unnecessary risk was created.

Since the security situation deteriorated, the security company was approached more openly to make sure the guards understood the risk Berghof was facing, so that they could deliver a more appropriate service. When our director's residence visa was revoked, we appreciated the close and trustful relationship with our security company and they helped us to deal with the uncomfortable uncertainty of what would happen next. Sharing sensitive information with security officers involves a certain discomfort as they frequently have a military or police background and because infiltrations by adversaries of conflict transformation cannot be ruled out completely. For Berghof, working constantly with a very limited number of security officers without rotation has proven to be useful. This facilitated building a relationship of trust that allowed us to share sensitive risk concerns.

Key lessons learned

- Making use of a security company as part of a deterrence strategy should be well thought through and its suitability depends on the context.
- If a security company is employed it should be approached openly, making sure they get an understanding of the specific risk situation.
- Working with a very limited number of security officers without rotation facilitates building a relationship of trust that allows sharing of sensitive risk concerns.

5. Dilemmas and controversial issues

Developing security performance for an organisation is always a work in progress and there will always remain dilemmas and controversial issues that need further consideration. We want to underline the following seven points that we had to deal with:

Planning security or managing security?

The security plan was an important document within the security architecture of Berghof in Sri Lanka but we have to bear in mind that the existence of a plan does not automatically lead to a good security performance. It is not possible to make plans for reactions to every single situation that could take place, and we learned that our approach to security had to be more holistic.

It is a common problem that security plans often become rather static documents disconnected from the actual work. The existence of a plan may lead even to an unrealistic sense of good practice in security: having “(...) such security plans may actually be an obstacle in achieving a real level of security while working in a violent environment: We need to manage security issues, instead of planning for them.” (Eguren 2000, p. 1)

How much risk is acceptable?

As a conflict transformation organisation working in a conflict area, Berghof bore an inherent risk that was directly related to our work. This risk we were facing was not constant but was changing due to dynamics in the political situation, due to the modifications in our work and due to threats and security incidents occurring to the organisation.

When analysing our risks we must ask ourselves: how much risk is acceptable? We could opt for a “security first” approach and take no risk at all, but then it would not be possible to carry out important activities or to pursue the aim of our organisation. There might be extreme situations when we need to decide to suspend our work, but usually the appropriate option is to keep on working while taking risks in a conscious way. Risk is something we can work with through regular and systematic risk analysis and monitoring. When the Government of Sri Lanka revoked our director’s residence visa without giving reasons we were worried

because of the uncertainty of this situation. What would happen next? Would other unexpected surprises follow? Would we be able to keep working until the announced office closure in July 2008 or would we be forced to close earlier? At this moment we took the decision to stay engaged but to monitor the situation by reviewing press articles regarding any further aggression and by observing the process of renewing residence visas for other Berghof personnel.

A frequent tendency is also to downplay risks, since we assume that the nature of working on conflict transformation implicates a certain risk and we do not want to appear scared of the adversaries. In this regard it is important to maintain a sensible level of awareness, by not taking uncalculated risks and allowing ourselves to acknowledge legitimate fears.

Aspects of internal team structure: differences in exposure and in nationality

The internal structure of an organisation is an important aspect that needs to be taken into consideration for a proper security performance.

On one hand there are differences in terms of exposure. Some team members are more exposed than others and their security needs special attention. In Berghof’s case the staff members from the most sensitive programme areas faced more risks than others and some were personally targeted. Apart from the security service offered by Berghof for all staff there was a particular service for these more vulnerable members, for example providing extra security guards and arranging transport. It was important to make the whole team aware about these differences in exposure, to make the need for a particular service understandable.

On the other hand there were differences in terms of nationality within the team. In general it is often criticized that the security needs of local staff do not figure highly in organisations’ security policies and that priority is given to expatriate staff (Stoddard et al 2006, p. 32). Berghof assumes that it is part of the responsibility of the organisation to treat the security of all staff members in a responsible way, without making any distinctions in terms of being local or expatriate. Basic measures like security training should be provided to

all staff members. We made efforts to carefully deal with situations of personal targeting, e.g. through providing alternative security arrangements during times of significant threat, or sending affected staff abroad to a foreign country for a certain time.

How to make a security sensitive selection of staff?

Making a sensitive selection of staff is essential for the security of an organisation. There are two key issues that need to be well considered: one is a balanced representation of ethnicities in the team and the second is the control of security gaps within the organisation.

Balanced representation of ethnicities within the team should be a standard for any international organisation engaged in transforming violent ethnopolitical conflicts, because it marks a contrast to practices of exclusion and discrimination. From a security perspective this balance has a particular importance because it is only through the representation and the contribution of different ethnicities that the organisation will be able to include information and perspectives from diverse sources in its risk analysis. In contrast, relying on a partial and incomplete perspective may lead to wrong interpretations and can even increase risk.

The staff selection process permits a certain space for the very sensitive task of controlling security gaps within the organisation. One possible method is to select only persons with an explicit social reference of having been engaged for a long time in conflict resolution efforts. The main disadvantage here is that it contradicts Berghof's approach of not recruiting staff from other conflict transformation organisations but instead getting new persons working in this field. Another method for the selection process is to question the candidates' stance on conflict transformation and their individual background. Blueprint solutions cannot be applied for the selection of staff, but it is essential to use discretion and sensitivity during the process.

Allocating resources for security

This point raises the question of how much of our resources, both in terms of time and money, we can and we want to invest in security? In fact activities such as

organising training sessions, implementing a new communication and media strategy and every other element of improving security all mean allocating resources for doing so.

Working in a context of violent conflict we have to realize the importance of the organisation's security, firstly because we have a responsibility for the staff members and secondly because we can only achieve our objectives if we know how to work with the risk we are facing. Therefore it is important that security expenses are part of the annual budget and that the corresponding time for security tasks is included in our work plans.

Will it increase our workload?

Introducing security measures and activities might provoke a feeling of increased workload among the team even if they are intended to achieve the opposite. This concern needs to be addressed by referring to the mutual relation between security measures and good programme implementation. Working on conflict transformation includes coping with risks and if we do not take security measures proactively, the implementation of our work will be limited. Addressing risks with an appropriate security management approach contributes to improving our work and avoids increasing workloads.

Maintaining alertness

After a long time without occurrences of real security incidents it becomes difficult to maintain an adequate level of alertness. In such situations security measures and procedures tend to decline and become less important for the team. But working on conflict requires continuous security activities, e.g. the risk assessment needs to be updated regularly to be able to detect new risks due to changes in the political situation. Apart from risks related to our work, we also needed to take into consideration the general situation of risk in a context such as Colombo, where bomb threats and road blocks occur frequently. An organisation needs mechanisms like a standing security committee to remind the team of the meaning and sense of security procedures and to call attention to remaining alert.

6. Reviewing strengths and challenges: what was successful and what needs to be improved

In the form of a short summary we want to identify the most significant strengths and weaknesses of our risk and security management. It aims to be a frank reflection, pointing out good practices and challenges.

Our strengths

Learning from our own experience

Besides the important input given to us in security training sessions and the use of helpful security manuals, we primarily developed our risk and security management out of practice, learning from the security incidents we experienced and responding to concrete needs. This way we were able to establish risk and security management that was appropriate for Berghof in Sri Lanka.

New communication and media strategy

The new communication and media strategy and the reorganisation of the communication unit were crucial for Berghof in Sri Lanka. Conflict transformation projects should consider carrying out proactive communication regarding their working principles and their activities from the first moment on.

Taking the security of local staff seriously

For Berghof it is essential to include local staff in all security procedures. The security services offered to our staff members did not differ on nationality but on the respective situation of threat and risk. In this sense, specific security measures were provided to particular targeted staff members, regardless of being local or expatriate.

Security is a team effort

For well-functioning risk and security management it is essential that the whole team is aware of the risks the organisation has to cope with. Through training sessions, simulations and special meetings, Berghof succeeded in making security an issue of discussion among staff members.

Sufficient time and resources for security issues

Since the deterioration of the security situation, Berghof allocated time and resources to establishing the security and risk management and to maintaining a security committee within the organisation. Additionally we dedicated resources for reviewing the process and for reflecting on lessons learned.

Our challenges

Proactive risk analysis

Regarding the analysis of risks it was difficult for Berghof to put theory into practice. While we were good at analysing security incidents in retrospect, we still needed to improve on analysing risks in a proactive way. In this sense it became important to systematically update the risk assessment and to draw conclusions for changes in work plans and strategies.

The security plan as an active resource

The whole Berghof team was involved since laying the foundations of our security plan during the initial security training, and subsequently the security committee made efforts to maintain a participatory process for establishing this plan. But it was a challenge to establish the security plan as an active resource for the team. To ensure more ownership we should have strengthened these efforts much more.

Coordination with other organisations

Apart from Berghof's discussion of security issues with other organisations, there is still no forum in Sri Lanka for organisations engaged in conflict transformation to coordinate on risk and security. We hope this learning case paper will serve as an opportunity to start disseminating and encouraging systematic exchange on security issues among conflict transformation organisations in Sri Lanka.

7. Bibliography

The following literature list is a selection of the most relevant reports and papers used for the elaboration of this learning case paper. Each text is briefly commented on.

ECHO (2004): Report on Security of Humanitarian Personnel. Standards and Practices for the Security of Humanitarian Personnel and Advocacy for Humanitarian Space. Brussels, Belgium.

[http://www.reliefweb.int/rw/lib.nsf/db900SID/LHON-66VEC8/\\$FILE/security_report_echo_2004.pdf?OpenElement](http://www.reliefweb.int/rw/lib.nsf/db900SID/LHON-66VEC8/$FILE/security_report_echo_2004.pdf?OpenElement)

(This report reviews how security is managed by different humanitarian organisations. It reflects experiences, reviews practices and indicates guidance on security issues.)

Eguren, Luis Enrique (2000): Beyond Security Planning: Towards a Model of Security Management. Coping with the Security Challenges of the Humanitarian Work. Journal of Humanitarian Assistance. Bradford, UK.

www.jha.ac/articles/ao60.pdf

(This short paper addresses the management aspect of security. It proposes an overall framework for a security management process allowing organisations to cope with security challenges.)

Eguren, Luis Enrique; Caraj, Marie (2008): New Protection Manual for Human Rights Defenders. Protection International (PI). Brussels, Belgium.

<http://www.protectionline.org/Protection-manual-for-human-rights.html>

(This manual is a practical resource for human rights defenders. It offers tools for analysing risks and threats and helps to define security and protection plans and strategies.)

Stoddard, Abby; Harmer, Adele; Haver, Katherine (2006): Providing Aid in Insecure Environments: Trends in Policy and Operations.

Overseas Development Institute (ODI)/ Humanitarian Policy Group (HPG) Report 23. London, UK.

<http://www.odi.org.uk/hpg/papers/hpgreport23.pdf>

(This report analyses the changing security environment for civilian operations and examines the related trends in policy and operations, in particular the development of security measures.)

Van Brabant, Koenraad (2000): Operational Security Management in Violent Environments. Overseas Development Institute (ODI)/ Humanitarian Practice Network (HPN) – Good Practice Review Report 8. London, UK.

<http://www.odihpn.org/download>.

[asp?id=2827&ItemURL=documents/gpr8/part1.pdf](http://www.odihpn.org/download.asp?id=2827&ItemURL=documents/gpr8/part1.pdf)

(This handbook is a practical reference tool offering a systematic step-by-step approach to security management. It explores a number of relevant crosscutting themes.)

Van Brabant, Koenraad (2001): Mainstreaming the Organisational Management of Safety and Security. A Review of Aid Agency Practices and a Guide for Management.

Overseas Development Institute (ODI)/ Humanitarian Policy Group (HPG) Report 9. London, UK.

www.odi.org.uk/HPG/papers/hpgreport9.pdf

(This report presents a comparative review of aid agencies' efforts to strengthen the management of safety and security and it provides tools for organisational managers.)

VENRO (2003): Minimum Standards Regarding Staff Security in Humanitarian Aid. Association of German Development Non-Governmental Organisations (VENRO). Bonn, Germany.

http://www.venro.org/fileadmin/Publikationen/english/personalsicherheit_engl.pdf

(This document offers practical advice for implementing minimum security standards, based on a review of a number of organisations' security documents and guidelines.)

All weblinks accessed 23rd December 2008.

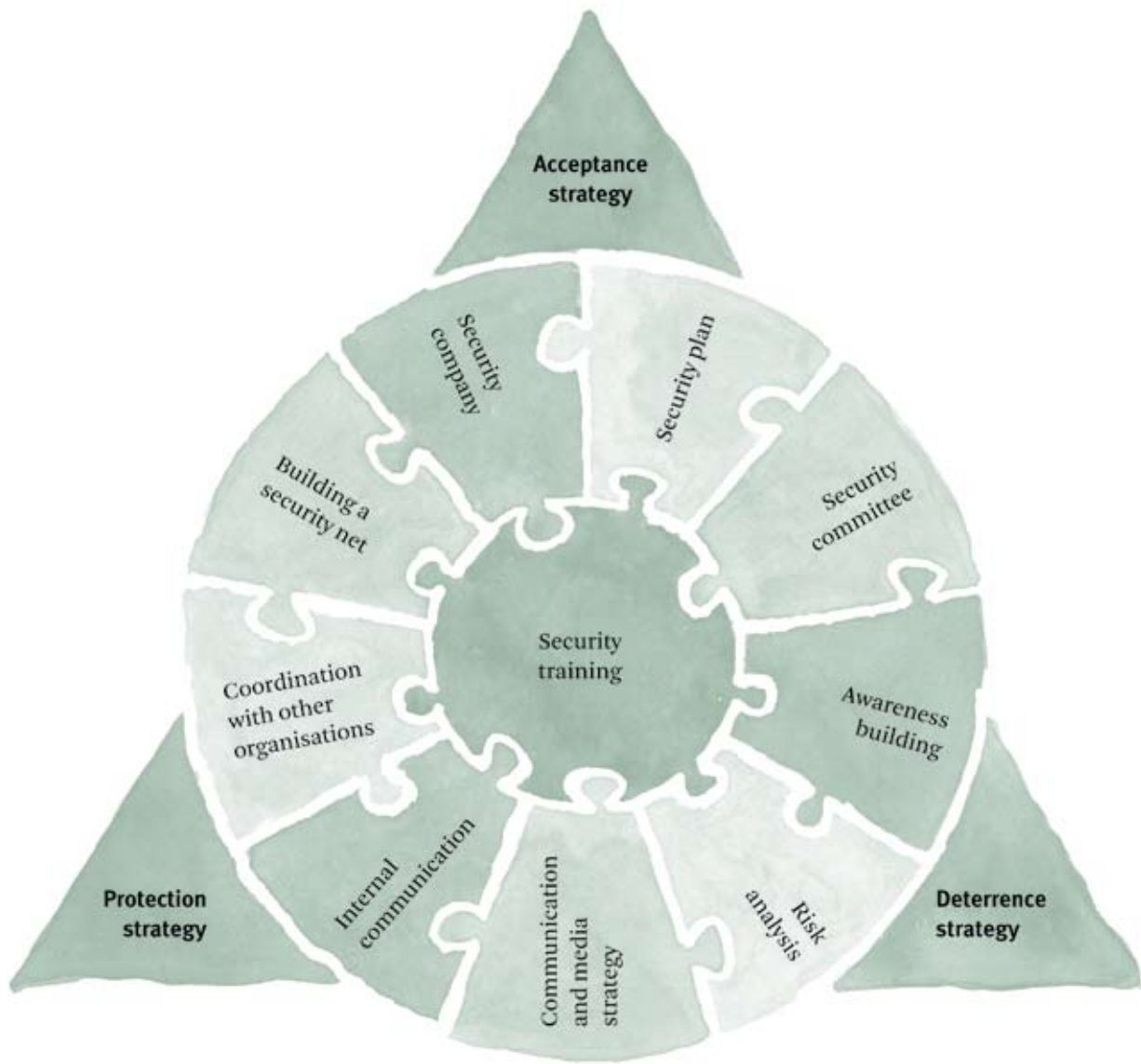


Diagramme: Berghof's risk and security management

Berghof Foundation for Peace Support

Berghof Foundation for Peace Support
Altensteinstr. 48a, 14195 Berlin, Germany
Phone +49 (0)30 844 154-0
Fax +49 (0)30 844 154 99
www.berghof-peacesupport.org
home@berghof-peacesupport.org

This learning case paper reflects the experience of the Berghof Foundation for Conflict Studies in Sri Lanka in establishing adequate risk and security management. It aims to share how we coped with a deteriorating security situation and outlines the adopted measures and activities. The core part of the document is the presentation of ten essential elements of Berghof's risk and security management. Remaining dilemmas and controversial issues are also highlighted and we complete this learning paper with reflections on the strengths and challenges of our security performance.