PROTECTION international

NEW PROTECTION MANUAL FOR HUMAN RIGHTS DEFENDERS

RESEARCHED AND WRITTEN BY ENRIQUE EGUREN AND MARIE CARAJ

New Protection Manual

for

Human Rights Defenders

Researched and written by Enrique Eguren,
and Marie Caraj, Protection International(PI)

Published by Protection International

Published by Protection International 2008
Rue de la Linière, 11
B-1060 Brussels, Belgium.

Printed copies of the *New* Manual from

Protection International
Rue de la Linière, 11. B-1060 Brussels (Belgium)
Tel: +32(0)2 609 44 05 / +32(0)2 609 44 07 / Fax: +32(0)2 609 44 07
pi@protectioninternational.org

It can be downloaded for free from **www.protectionline.org**

Prices of printed copies:

Southern organisations: free

Northern organisations: 20 Euros plus post and packaging (reductions for bulk orders)

The *New* manual is available in English, French and Spanish (it is also being translated into other languages by Protection International)

ISBN: 978-2-930539-00-3

Foreword to the first edition by Hina Jilani

In my work as Special Representative of the Secretary General on Human Rights Defenders I have noted with grave concern an increase in the number of reports of serious human rights abuses against defenders and a notable shift away from low-targeting, such as intimidation and harassment, to more serious violations, such as attacks on and threats to physical integrity of defenders. In 2004 we worked on reports of at least 47 defenders who had been killed because of their work.

It is clear that the primary responsibility for the protection of human rights defenders lies with Governments, as set out in the UN Declaration on Human Rights Defenders[1]*. We must continue to work to get all governments to take seriously their obligations in this regard and take effective measures to ensure protection of human rights defenders.*

However, the gravity of the risks faced on a daily basis by human rights defenders is such that it is also important to pursue other means to strengthen their protection. In this regard I hope that this Protection Manual will support human rights defenders in developing their own security plans and protection mechanisms. Many human rights defenders are so engaged by their work to protect others that they give insufficient attention to their own security. It is important that all of us involved in working for human rights understand that we must be concerned about security for ourselves and for the people we work with and for.

Hina Jilani
Former UN Secretary-General's Special Representative on Human Rights Defenders

[1] Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Respect Universally Recognised Human Rights and Fundamental Freedoms.

Protection International -PI-

PI members have over 25 years' combined experience in the protection of human rights defenders and other vulnerable groups. PI members' experience originates from their former involvement and participation in Peace Brigades International -PBI[1]- and other international organisations.

PI aims to contribute to the fulfilment of national and international obligations for the protection of defenders. Many NGOs and institutions already work on human rights and defenders issues. PI intends to complement this work.

PI's global strategy for the protection of defenders includes:

Protection and security capacity building and training

- Risk assessment, security/ protection management.
- Transfer of knowledge and tools.

  Publication of manuals, among which this *New* Manual (and its previous edition[2])
  Training: between 2004-2008 over 1700 defenders have participated in PI capacity building and security workshops, improving their capacities in the management of their own security and their protection of others.

Protection research

- Study and elaboration of protection/security operational tools.
- Publication of information on the basis of lessons learned and best practices.

Protection advocacy

- Distribution of information on protection among HRD, IDP, EU institutions and EU Member States in the form of recommendations, reports and press releases and documentaries.
- Reminding both national and international authorities of their international obligations with regard to the protection of HRD, IDP, refugees and other social actors.
- Promotion of debates and action to protect HRD; involvement of parliaments, trade unions and the media.

Protection video (video advocacy)

- Portraits of Human Rights Defenders.

[1] As of 25th October 2007, by royal decree of the Federal Public Justice Service, the European Bureau of Peace Brigades International, through the amendment of its articles published in the Belgian Official Journal, became "Protection International", an international non-profit making association

[2] With the financial support of Front Line and the Development Cooperation of Ireland.

Protection desk

- In partnership with local HRD networks, protection desks are set up as national and regional centres for protection and security management.
- Progressive hand-over to PD of the whole process of security/protection management (ownership is part of that process).

Protectionline

- www.protectionline.org is a one-stop website by/with/for HRD and those seeking to contribute to HRD protection.
- Daily update of information, documents, publications, testimonies, urgent actions and tools designed to promote the protection of HRD.

Normative framework:

PI follows all international standards in international human rights and humanitarian law. Specifically, PI will use the guidelines provided by the UN Declaration on Human Rights Defenders (1998), and the EU Guidelines on HRD (2004), as well as the resolutions on defenders promoted by PI and adopted by EU member states in Spain, Belgium and Germany.

PI CAPACITY BUILDING AND SECURITY WORKSHOPS

From 2004 through 2007, a total of 1747 human rights defenders have participated in PI capacity building and security workshops.

- In South and Central America: 558 HRD
  (Bolivia, Brazil, Colombia, Guatemala, Honduras, México, Perú)
- In Asia: 650 HRD
  (Burma, Indonesia, Nepal, Thailand)
- In Africa: 441 HRD
  (Kenya, Uganda, Democratic Republic of Congo)
- In Europe: 98 HRD
  (Germany, Belgium, Ireland, Serbia, Republic of Ingushetia)

HRDs often protect others whilst neglecting their own security. There are various reasons for this. PI training in security and protection deals with these reasons and allows time to reflect on the risks and threats of which HRDs are the target. PI training enables a detailed breakdown of risks and also the know-how and logic needed to incorporate security into HRDs' work plans. During training, security is broken down into its different elements so as to analyse them, reflect on possible theories, scenarios and probable consequences of specific choices, and then choose the option whose consequences the HRDs believe they can manage, fully aware that they cannot be sure of a specific outcome.

In any case there is no magic answer that works every time; training aims to ensure that HRDs acquire the skills needed for security: analysis, outcome, management and updating of the process. They have to do this on an individual, organisational and inter-organisational level, taking into account at least the political, psychosocial and physical exposure.

Preface

After over a decade of training, research and meetings with human rights defenders and other stakeholders responsible for human rights defenders' protection, we at Protection International have decided to renew our tribute to defenders and once again to include their contributions into this new protection manual written with, from, by, for all human rights defenders.
In the last three years, Protection International has developed further its training and research, benefiting from field experience and feedback from human rights defenders.

In the new manual, Protection International is putting forward management logic that can be taken up in different organisational environments and structures, arriving at the same outcome: the incorporation of the security plan into the work plan. There is no magic answer, merely choices and consequences to manage. This can be achieved through brainstorming, asking the right questions, carrying out risk and organisational security assessments, drafting inclusive plans and processes…

This new manual thereby aims at ownership by human rights defenders of the whole security-protection logic and process. Ownership is a component of security itself. The new manual contributes to independence and sustainability of security-protection of human rights defenders.

Although there is no "one size fits all" security plan, the new manual transcends differences in cultural, social, religious, organisational context and structures. The manual can easily be used by human rights defenders to tailor make their security-protection as we are aware that they have the essential fabric: knowledge and experience of their own context.

Protection International differentiates between the security of the human rights defenders– towards him/herself– and the protection of the human rights defender - from other stakeholders towards the human rights defender.

Acknowledgment:

- The updated and extended new version and new edition of the manual is the result of the contribution of

  - all human rights defenders who have so far attended Protection International trainings in security-protection management. It is impossible to list all of them here. They are located in Bolivia, Brazil, Burma Colombia, Democratic Republic of Congo, Guatemala, Honduras, Indonesia, Ingushetia, Kenya, Mexico, Nepal, Peru, Serbia, Sri Lanka, Thailand, Uganda.

  - PI current and previous members: Pascale Boosten, Soledad Briones, Shaun Kirven, Christoph Klotz, Rainer Mueller, Michael Schools

  PI's current and previous collaborators: Ana Cornide, Jérôme Hieber, Eric Juzen, Maria Martin, Thomas Noirfalisse, Sheila Pais, Flora Petrucci, Sophie Roudil, Catherine Wielant, Jabier Zabala…

• Carmen Díez and Montserrat Muñoz who both took utmost care of the design and DTP of the previous and current editions of the Manual. Thomas Noirfalisse contributed with his design of PI logo and ideas for the cover design.

Warm thought to Brigitte Scherer.

Acknowledgement to Peace Brigades International and more than two decades of shared experience.

We are grateful to the support of the *Bundeministerium für Wirtschaftliche Zusammenarbeit und Entwicklung* (German Ministry for Cooperation and Development) and the *Service public fédéral Affaires Etrangères Belgique* (Belgian Foreign Affairs Public Service)

The *New* Protection Manual for Human Rights defenders updates and extends the first Manual Protection for Human Rights Defenders (author: Luis Enrique Eguren © 2005 PI former PBI-BEO) which was published with the financial support of Front Line and of the Development Cooperation of Ireland.

The draft of the first manual was commented by Arnold Tsunga (Zimbabwe, Lawyers for Human Rights), Sihem Bensedrine (Tunis, Conseil National pour les Libertés en Tunisie), Father Bendan Forde (Colombia, Itinerant Franciscans,), Indai Sajor (Philippines, former Director of the Asian Centre for Human Rights), James Cavallaro (Brazil, Associate Director of human Rights Programme – Harvard Law School), Nadejda Marques (Brazil, Consultant and Researcher - Global Justice) and Marie Caraj (PI former PBI BEO)

Other colleagues have contributed with their own work: José Cruz and Iduvina from SEDEM (Guatemala), Jaime Prieto (Colombia), Emma Eastwood (UK) and Cintia Lavandera at the Human Rights Defenders Programme from Amnesty International in London.

The Human Rights Defenders Program from Amnesty International in London and the Indonesia Project of PBI provided the funds for translations of the first edition of the manual into Portuguese and Indonesian respectively. The International Commission of Jurists translated it into Thai, and PBI into Nepalese.

Chapter 2.11 is based on the work of Robert Guerra, Katitza Rodriguez and Caryn Madden from Privaterra (Canada).

Acknowledgments from the author: Luis Enrique Eguren

Also many other people have contributed to gathering the background knowledge necessary for writing the Manual, that it is impossible to list all of them here. I would like to mention just few names, such as:

To all the PBI people, and specially to my former close colleagues in the Colombia Project such as Marga, Elena, Francesc, Emma, Tomás, Juan, Mikel, Solveig, Mirjam, Jacobo and so many others…

To Danilo, Clemencia and Abilio and their colleagues from the *Comision Intereclesial de Justicia y Paz* in Colombia. They taught to me how to live inside the heart of the people.

To the people of Santa Marta, in El Salvador, and of Cacarica, Jiguamiando and San Jose de Apartado in Colombia. They, among others, taught to me how people in the countryside live with dignity.

To Irma Ortiz, co-trainer in many workshops, and all the other colleagues at *Pensamiento y Acción Social* (PAS) in Colombia.

For the advice and initial knowledge provided by REDR (London) and Koenraad van Brabant (Belgium).

And to the many defenders met in El Salvador, Guatemala, Colombia, Mexico, Perú, Bolivia, Burma, Sri Lanka, Croatia, Serbia, Kosovo, Rwanda, Democratic Republic of Congo, Ingushetia, etc. An ocean of conversations, tears, smiles and learning and commitment….

Finally, nothing would have been possible without the love and dedication and support of Grisela and Iker and my parents. All my love to them.

Acknowledgments from the co-author: Marie Caraj

I feel admiration, respect, solidarity, empathy and gratefulness for every single human defender I have met, will meet and will never meet. They have changed my life. The days spent together have, imperceptibly, forged a bond between us.

I am torn between anger against human rights violators and hope that one day they will see that they are not being discriminated against by human rights defenders and may safely join the movement towards the time when all human rights will be respected and defenders are able to enjoy a normal life.

To Leze Gegaj, my mother, the first woman human right defender I met.

To all my friends and colleagues for their tacit or explicit support. Most of them have shared the stories I brought back and have helped to recharge my batteries.

We thank all of the above mentioned, and the many more human rights defenders we have worked with and learned from, for their input. Any errors remaining in this *New* Manual (although we have done our utmost for there not to be any left!) are entirely due to proofreading oversights by us. We hope that the new manual will be a useful tool in improving the protection and security of human rights defenders, although we realise that it provides no guarantees and that ultimately on these issues everyone must take responsibility for themselves. We look forward to your feedback.

Protection International
February 2008

Disclaimer

New security and protection manual for human rights defenders

Human rights defenders at risk

Human Rights are guaranteed under international law but working to ensure that they are realised and taking up the cases of those who have had their rights violated can be a dangerous activity in countries all around the world. Human Rights Defenders are often the only force standing between ordinary people and the unbridled power of the state. They are vital to the development of democratic processes and institutions, ending impunity and the promotion and protection of human rights.

Human Rights Defenders often face harassment, detention, torture, defamation, suspension from their employment, denial of freedom of movement and difficulty in obtaining legal recognition for their associations. In some countries they are killed, abducted or "disappeared."

Over the last few years, general awareness has increased of the enormous risk human rights defenders face in their work. The risk is easy to identify when defenders work in hostile situations, for instance, if a country's laws penalise people who do certain types of human rights work. Defenders are also at risk when the law fully sanctions human rights work on the one hand, but fails to punish those who threaten or attack defenders on the other. In armed conflict situations, the risk becomes even higher.

Apart from a few chaotic situations during which a defender's life may be in the hands of soldiers at a checkpoint, the violence committed against defenders can't be called indiscriminate. In most cases, violent attacks are a deliberate and well-planned response to defenders' work, and linked to a clear political or military agenda.

These challenges require human rights defenders to implement comprehensive and dynamic security strategies in their day- to- day work. Giving defenders well-meant advice or recommending that they "take care" is not enough. Better security management is key. This manual does not offer tailor-made solutions ready to be applied to any scenario. However, it does try to provide a set of strategies aimed at improving defenders' security management.

The most effective security lessons come from defenders themselves - from their daily experiences and the tactics and strategies they develop over time in order to protect others and their own working environments. This manual must therefore be understood as a work in progress which will need to be updated and adapted as we gather more input from human rights defenders.

There are also lessons to be learned from international humanitarian NGOs, who have recently started to develop their own rules and procedures to maintain staff security.

It is important to be aware that the main risk for defenders is that threats often materialise into actual attacks. Aggressors have the will, the means and the impunity to put threats into action. The best tool for protecting defenders is therefore political action to address the one, big, remaining issue: the need for governments and civil society to put pressure on and act against those who day after day threaten, harass and kill defenders. The advice given in this manual is in no way intended to replace the due responsibility of each and all governments to protect human rights defenders.

That said, defenders can significantly improve their security by following a few tried and tested rules and procedures.

This manual is a humble contribution to an aim shared by many different organisations: to preserve the invaluable work that human rights defenders do. They are the primary stakeholders and they are also the main protagonists in this manual.

The manual

The purpose of this manual is to provide human rights defenders with additional knowledge and some tools that may be useful for improving their understanding of security and protection. It is hoped that the manual will support training on security and protection and will help defenders to undertake their own risk assessments and define security rules and procedures which suit their particular situation.

This manual is the result of over 25 years combined experience of Protection International-PI- members in working with human rights and humanitarian law and in the protection of HRD and other vulnerable groups. PI members experience originates from their former involvement and participation in Peace Brigades International – PBI-field missions and structure.

We have had the opportunity to learn from and share experiences and knowledge with hundreds of defenders in the field, as well as in workshops, meetings and discussions about security. Most of the manual's contents have already been applied in practice, either in protection work or in training workshops with defenders. This manual is the fruit of all these exchanges, and we owe the defenders involved a huge thanks for their input.

Security and protection are complex areas. They are based around structured knowledge, but also influenced by individual attitudes and organisational beha-

viour. One of the key messages in this manual is to give the issue of security the time, space and energy it deserves, despite overloaded work agendas and the severe stress and fear all defenders and their organisations are under. This means going beyond people's individual knowledge about security and moving towards an organisational culture in which security is inherent.

Knowing enough about a conflict scenario and understanding the local political logic are also key to proper management of defenders' security. This manual contains an overall framework as well as a step- by- step approach to draw a security plan (product) and to to manage security (process). It includes some thoughts on basic concepts like risk, vulnerability and threat, and a few suggestions for how to improve and develop security for defenders in their day- to- day work. We hope that the topics covered will allow NGOs and defenders to plan for and tackle the increasing security challenges involved in human rights work.

This said, the first thing we wish to call to mind is that defenders risk their well-being and their lives, and this is serious matter. Sometimes the only way to save a life is by going into hiding and then fleeing. We want to make it very clear that all the techniques and suggestions in this manual are not, by any means, the only way to think about security issues for defenders. The manual has been written in good faith but sadly offers no guarantee of success.

Let's improve this Manual...

Risk changes. The manual is a work in progress, and will need to be developed, improved and refined over time. Your feedback as a defender on any aspect of this manual will be invaluable.

Please send any comments and opinions - particularly in terms of your experiences of using the manual in your work. With your help, we can make this manual an increasingly useful tool for defenders all over the world.

Email to any of us:

pi@protectioninternational.org

Or by post to PI

Protection International. Rue de la Linière, 11 - 1060 Bruxelles (Belgium)
Tel : + 32 (0)2 609 44 05, +32 (0)2 609 44 07
Fax: +32 (0)2 609 44 06

www.protectioninternational.org

www.protectionline.org

A short introduction to Human Rights Defenders.

"Human rights defender" is a term used to describe people who, individually or with others, take action to promote or protect human rights. Human rights defenders are identified above all by what they do, and the term can therefore best be explained by describing their actions and some of the contexts they work in.

Human rights defenders' work is legal and legitimated by the civil society they represent.

Every day around the world hundreds of Human rights defenders are exposed to political violence due to their defense of the rights of others. Risking their own physical and mental integrity, they strive to bring an end to impunity of human rights violations and to promote social justice and peace.

In 1998 the United National General Assembly approved the "Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms" (Hereafter the "UN Declaration on Human Rights Defenders"). In other words, fifty years after the Universal Declaration of Human Rights, and after twenty years of negotiations on a draft declaration on human rights defenders, the United Nations finally recognized what is a reality: that thousands of people were promoting and contributing to the protection of human rights throughout the world. This is an inclusive Declaration that honours the amount and variety of people engaged in the promotion and protection of human rights.

Originally, the position of The Special Representative of the UN Secretary General on Human Rights Defenders was created "to seek, receive examine and respond to information on the situation and the rights of anyone, acting individually or in association with others, to promote and protect human rights and fundamental freedoms." In 2008 it was substituted by the position of UN Special Reporter on Human Rights Defenders.

The European Union –EU- Guidelines on Human Rights Defenders (2004) not only have integrated the entire UN Declaration on Human Rights Defenders but they also give specific recommendations to EU Member States –MS-.

Human rights defenders are legal and legitimated by international and national communities. PI subscribes to the definition of who is a human rights defender provided by the UN Declaration on Human Rights Defenders and reiterated by the EU Guidelines on Human Rights Defenders:

> "Human rights defender is a term used to describe people who, individually or with others, act to promote or protect human rights. Human rights defenders are identified above all by what they do and it is through a description of their actions and of some of the contexts in which they work at the term can bes be explained"1.

(See in the appendix at the end of the manual for more information on the UN Declaration on HRD and on the EU Guidelines on HRD)

[1]Human Rights Defenders: Protecting the Right to Defend Human Rights. Fact Sheet No. 29. www.unhchr.ch

Who is responsible for protecting human rights defenders?

The Declaration on Human Rights Defenders stresses that the state is primarily responsible for protecting human rights defenders. It also acknowledges *"the valuable work of individuals, groups and associations in contributing to the effective elimination of all violations of human rights and fundamental freedoms" and "the relationship between international peace and security and the enjoyment of human rights and fundamental freedoms".*

But according to Hina Jilani, former Special Representative of the UN General Secretary on Human Rights Defenders, "exposing human rights violations and seeking redress for them is largely dependent on the degree of security enjoyed by human rights defenders"[2]. A look at any report on human rights defenders throughout the world reveals stories of torture, disappearances, killings, threats, robbery, break-ins to offices, harassment, illegal detentions, being subjected to intelligence and surveillance activities, etc. Unfortunately, this is the rule and not the exception for defenders.

Suggested further reading

To find out more about human rights defenders, visit:

- www.unhchr.ch/defender/about1.htm (The UN High Commissioner on Human Rights).
- www.protectionline.org (Protection International)
- The Observatory for the Protection of Human Rights Defenders, created by the International Federation on Human Rights (FIDH; www.fidh.org) and the World Organisation Against Torture (OMCT; www.omct.org).
- Amnesty International: www.amnesty.org and http://web.amnesty.org/pages/hrd-index-eng
- www.ishr.ch, see under "HRDO" (The HRD Office of the International Service for Human Rights in Geneva)
- www.frontlinedefenders.org (Front Line, The International Foundation for Human Rights Defenders)

To learn more about existing international legal instruments and the UN Declaration on Human Rights Defenders, visit :

- www.unhchr.ch : this is the web site of the UN High Commissioner for Human Rights.
- www.protectionline.org (Protection International)
- www.ishr.ch/index.htm (International Service for Human Rights, Geneva), for a compilation of international and regional instruments for the protection of human rights defenders.

[2]Report on Human Rights Defenders, 10 Sept 2001 (A/56/341)

PART I

RISK, THREAT ASSESSMENT AND OTHER TOOLS

In first part of this Manual we are covering the basic security concepts, some practical tools and security approaches to some specific cases.

All of them will be integrated in the security plan and security manual of the organisation.

CONTENTS OF FIRST PART:

CHAPTER 1.1

Making informed decisions about security and protection

Purpose:

To become aware of the importance of analysing your working environment for security reasons.

To learn different methods for undertaking context and stakeholder analyses.

Human rights defenders' working environments

Human rights defenders usually work in complex environments, where there are many different actors, and which are influenced by deeply political decision-making processes. Many things will be happening almost simultaneously, with each event impacting on another. The dynamics of each actor, or stakeholder, in this scenario will play a significant role in that actor's relationships with others. Human rights defenders therefore need information not only about issues directly related to their work, but also about the positions of key actors and stakeholders.

A first, simple exercise would be to organize a group brainstorming to try to identify and list all the social, political and economic actors that may have an influence on your current security situation.

Analysing your working environment

It is very important to know and understand as much as possible about the context you are working in. A good analysis of that context enables informed decisions about which security rules and procedures to apply. It is also important to think about possible future scenarios, in order, where possible, to take preventive action.

However, simply analysing your working environment isn't enough. You also need to look at how each intervention could affect the situation and how each actor might react. It is also important to take into account the extension of a work space. You can undertake an analysis at **macro** level by studying a country or a region, but you also have to find out how those macro dynamics function in the particular area where you are working, i.e. the **micro** dynamics.

For instance, paramilitaries in one local area may act differently to how you might expect following a regional or national analysis. You need to be aware of such local characteristics. It is also crucial to avoid having a fixed view of a work scenario, because situations evolve and change. They should therefore be reviewed regularly.

Asking Questions, the ***Force Field Analysis*** and the ***Stakeholder Analysis*** are three useful methods for analysing your working environment:

Asking questions

You can understand your working environment better simply by asking the right questions about it. This is a useful tool for generating discussions in a small group, but it will only work if the questions are formulated in a way that will make it easy to find a solution.

Suppose, for example, that harassment by local authorities has become a problem. If you phrase the question as: "What should be done to reduce the harassment?", you may find yourselves simply looking for a remedy to a symptom, i.e. the harassment.

But if you phrase the question to point toward a solution, you may be on your way to finding a real solution. For example, if you ask: "Is our socio-political environment safe enough for doing our work?", there can be only two answers – yes or no.

If the answer is yes, you will need to formulate another question that can help you pin-point and properly understand the critical issues at stake for maintaining your safety. If, after proper consideration of all available activities, plans and resources, as well as legislation, negotiations, comparisons with other defenders in the area, etc, the answer should turn out to be no, this in itself will amount to a solution to your security problem.

Using the Asking Questions method:

- Look for questions that will help you pin-point and properly understand the critical issues at stake for maintaining your safety;
- Formulate the questions in a solution-oriented way;
- Repeat this process as many times as necessary (as a discussion).

Some useful questions to be asked:

- Which are the key issues at stake in the socio-political and economic arena?
- Who are the key stakeholders in relation to these key issues?
- How might our work affect negatively or positively the interests of these key stakeholders?
- How might we react if we became targeted by any of these actors due to our work?

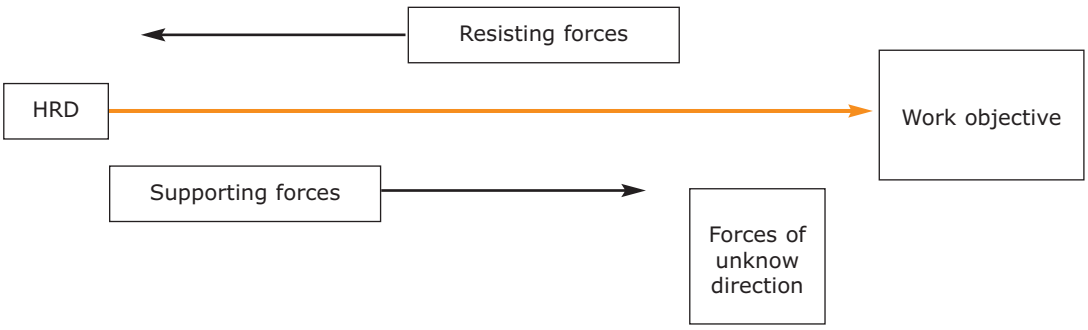
- Is our socio-political environment safe enough for doing our work?
- How have local/national authorities responded to previous work of rights defenders related to this issue?
- How have the key stakeholders responded to previous or similar work of rights defenders or others related to these issues?
- How have the media and the community responded in similar circumstances?
- Etc.

Force Field Analysis

Force field analysis is a technique which can help you visually identify how different forces are helping or hindering the achievement of your work objectives. It shows both supporting and resisting forces, and works on the assumption that security problems might arise from resisting forces, and that you could take advantage of some of the supporting forces. This technique can be completed by just one person, but is most effective when used by a diverse group with a clearly defined work objective and a method for accomplishing it.

Begin by drawing a horizontal arrow pointing to a box (you working towards your objective). Write a short summary of your work objective in this box. This will provide a focus for identifying supporting and resisting forces. Draw another box above the central arrow. List all potential forces which could be preventing you from achieving your work objective here. Draw a similar box, containing all potential supportive forces, underneath the arrow. Draw a final box for forces whose direction is unknown or unsure.

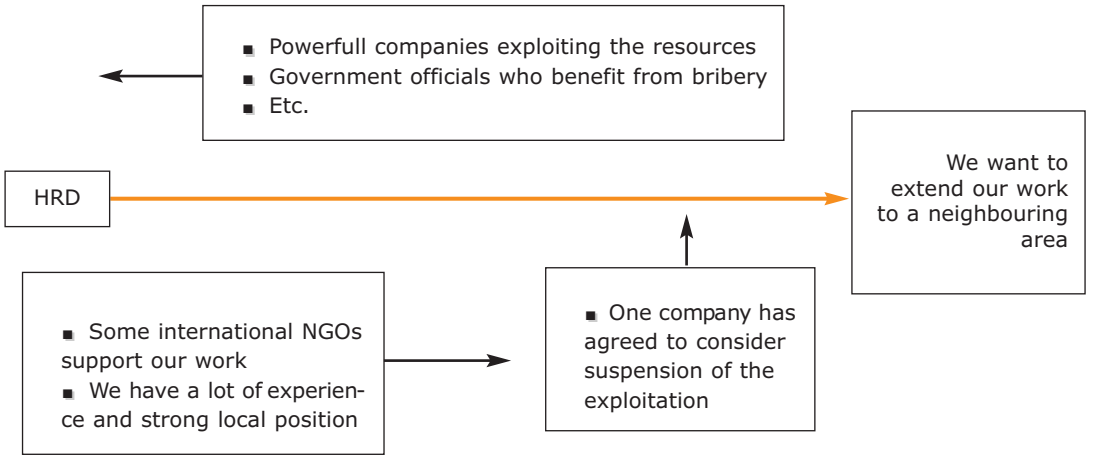
Chart 1: Force field analysis for assessing working environments



After completing your chart it is time to evaluate the results. Force field analysis helps you to clearly visualise the forces you are dealing with. The goal is to find ways to reduce or eliminate risk generated by resisting forces, partly through potential help from supporting forces. In terms of the forces of unknown direction, you will need to decide whether to look at them as supporting, or to monitor them continuously in order to detect signs of them becoming either resisting or supporting.

For example:

Imagine that you belong to an organisation dealing with indigenous people's rights to natural resources on their own land. There are ongoing conflicts between a number of stakeholders about the exploitation of those resources. You now want to extend your work to a neighbouring area with similar problems.



Actors (or stakeholders) Analysis

Actors or stakeholder analysis is an important way of increasing the information you have available when making decisions about protection. It involves identifying and describing the different actors or stakeholders involved and their relationships, on the basis of their characteristics and interests – all in relation to a given protection issue.

A stakeholder in protection is any person, group or institution with an interest in, or involvement in, a policy outcome in the area of protection[1].

Stakeholders in protection can be categorised in the following way:

Primary stakeholders. In a protection context, these are **the defenders themselves, and those they work with and for**, because they all have a primary stake in their own protection.

[1] Adapted from *Sustainable Livelihoods Guidance Sheets* No. 5.4 (2000)

Duty-bearer stakeholders, who are responsible for protecting defenders, i.e.:

- Government and state institutions (including security forces, judges, legislators, etc)
- International bodies with a mandate that includes protection, such as some UN bodies, regional IGOs, peacekeeping forces, etc;
- In the case of opposition armed actors, they can be held accountable for not attacking the defenders (as they are civilians), especially when these actors control the territory.

Key stakeholders, who can significantly influence the protection of defenders. They may have political clout or the capacity to put pressure on duty-bearer stakeholders who do not fulfil their responsibilities (such as other governments, UN bodies, etc), and similarly some of them may be often directly or indirectly involved in attacks and pressure against defenders (such as private corporations, the mass media or other governments). It depends on the context, interests and strategies of each of these key stakeholders. A non-exhaustive list could include:

- UN bodies (other than mandated ones);
- The International Committee of the Red Cross (ICRC);
- Other governments and multilateral institutions (both as donors and policy-makers);
- Other armed actors.
- NGOs (either national or international);
- Churches and religious institutions;
- Private corporations;
- The mass media

A major difficulty with establishing which strategies and actions are being undertaken by stakeholders is that the relationships between them are not clear-cut, or may even be non-existent. Many duty-bearer stakeholders, particularly governments, security forces and opposition armed forces, cause or contribute to human rights violations and a lack of protection for defenders. Some stakeholders, who would otherwise share the same protection concerns, may also have competing interests, such as other governments, UN bodies and NGOs. These factors, along with those inherent in conflict scenarios, project a complex picture of the working environment as a whole.

Analysing changing stakeholders, structures and processes

Stakeholders are **not static** actors. They relate to each other at multiple levels, creating a dense web of relationships. It is important to pay attention to relationships which shape and transform people's protection needs.

Structures are interrelated parts of the public sector, civil society or private bodies. We will look at them from the point of view of protection. Within the public sector, we could look at a government as a set of actors with either one unified stra-tegy or with confronting internal strategies. For example, we could find strong discrepancies between the Ministry of Defence and the Ministry of Foreign Affairs when discussing policies related to human rights defenders, or between the Ombudsman's office and the military. Structures can have mixed components; for example, an inter-sectoral commission (members from the government, NGOs, the UN and diplomatic corps) could be created to monitor the protection situation of a given human rights defenders organisation.

Processes are the chains of decisions and actions taken by one or more structures with the goal of improving the protection situation of a given group. They can be legislative processes, cultural processes and policy processes. Not all processes are successful in achieving improvements in protection: On many occasions protection processes are in conflict or render each other ineffective. For example, people allegedly being protected may not accept a policy protection process led by the government, because they see it as having an implicit aim of displacing people from an area. The UN and NGOs may support people in this process.

A stakeholder analysis is key to understand:

- who is a stakeholder and under what circumstances their "stake" counts;
- the relationships between stakeholders in protection, their characteristics and interests;
- how these will be affected by protection activities;
- each stakeholder's willingness to become involved in those protection activities.

There are a number of ways to do a stakeholder analysis. The following uses a straight-forward methodology, which is key to getting good results.

When assessing protection processes it is important to look at them with an adequate time perspective and always take into account the interests and objectives of all stakeholders involved.

A stakeholder analysis in four steps:

1. Identify the wider protection issue (i.e. the security situation of human rights defenders in a given region within a country).

2. Who are the stakeholders? (Namely, which are the institutions and groups and individuals with a responsibility or an interest in protection?) Identify and list all stakeholders relevant to that protection issue, through brainstorming and discussion.

3. Analyse the stakeholders' characteristics and particular attributes, such as responsibilities in protection, the power to influence the protection situation, aims, strategies, legitimacy and interests (including the will to contribute to protection).

4. Investigate and analyse relationships between stakeholders.

After undertaking this analysis, you may wish to use a matrix like the following.

Place the list with all stakeholders relevant to a well-defined protection issue in a matrix (see Chart 1.2): Repeat the same stakeholders list in the first column and along the first row. Next:

- Analyse the attributes of each stakeholder (aims and interests, strategies, legitimacy and power), fill in the boxes in the diagonal line where each stakeholder intersects with itself:

For example:

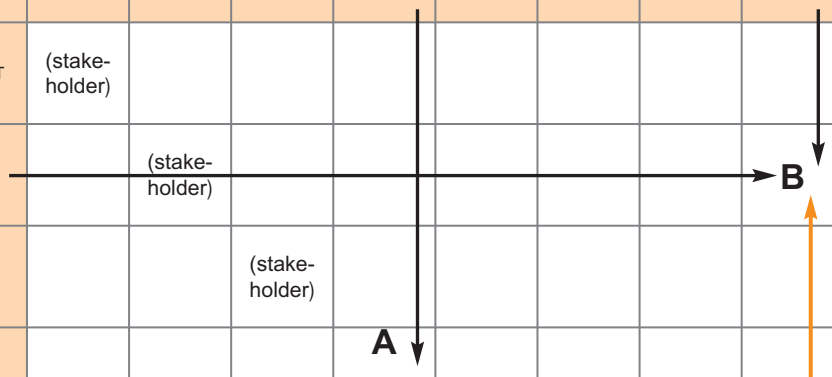
Place the aims, interests and strategies of armed opposition groups in the box "A".

- Analyse the relationships between stakeholders, fill in the boxes that define the most important relationships in relation to the protection issue, for example, the one which intersects between the army and the United Nations High Commissioner for Refugees (UNHCR), in box "B", and so on.

After filling in the most relevant boxes, you will have a picture of the aims and strategies and interaction among the main stakeholders in relation to a given protection issue.

Chart 2: A matrix system for stakeholder analysis

	Government	Army	Police	Armed opposition group	National human rights NGOs	Churches	Other governments	UN agencies	International NGO
Government	(stakeholder)								
Army		(stakeholder)							
Police			(stakeholder)						
Armed opposition groups									
National human rights NGOs					(stakeholder)				
Churches						(stakeholder)			
Other governments							(stakeholder)		
UN agencies								(stakeholder)	
International NGOs									(stakeholder)



Box "**A**"

For each stakeholder:

- aims and interests
- strategies
- legitimacy
- power

Box "**B**"

Interrelationship between stakeholders:

(Interrelationship in relation to the protection issue and in relation to strategic issues for both stakeholders)

Summary

- All human rights defenders face risks
- Not all human rights defenders are equal in front of risks
- Risks depend on the political context.
- The political context changes, it is dynamic.
- Thus, the risk is dynamic.

This is the hypothesis on which we base the importance of finding key information by asking the right questions.

Then, map and analyse the stakeholders with all their components up to their deepest many sub-strata.

Establish how they all interact as to protection issues and how the latter relate to stakeholder's strategic issues.

Find converging and diverging interests, alliances, operational methods etc.

See what are the underlying structures and processes.

You will be able to pinpoint the different forces (resisting, supporting and of unknown direction)

The first time through the above steps can be demanding. Then, if your analysis is updated regularly, it is far easier

This will help you making informed decisions about security and protection.

CHAPTER 1.2

Assessing risk: threats, vulnerabilities and capacities

Purpose:

Understanding the concepts of threats, vulnerability and capacity in security.

Learning how to do a risk assessment.

Risk analysis and protection needs

Human rights defenders' work can have a negative impact on specific actors' interests, and this can in turn put defenders at risk. It is therefore important to stress that **risk is an inherent part of defenders' lives in certain countries.**

The issue of risk can be broken down in the following way:

> Analyse main stakeholders' interests and strategies ⇨ Assess impact of defenders' work on those interests and strategies ⇨ Assess threat against defenders ⇨ Assess vulnerabilities and capacities of defenders ⇨ Establish Risk.

In other words, the work you do as a defender may increase the risk you face.

- **What** you do can lead to threats
- **How**, **where**, and **when** you work raises issues about your vulnerabilities and capacities.

There is no widely accepted definition of risk, but we can say that risk refers to possible events, however uncertain, that result in harm.

In any given situation, everyone working on human rights may face a common level of danger, but not everyone is equally vulnerable to that general risk just by being in the same place. **Vulnerability** - the possibility that a defender or a group will suffer an attack or harm - varies according to several factors, as we will now see.

An example:

There may be a country where the Government poses a general threat against all kinds of human rights work. This means that all defenders could be at risk. But we also know that some defenders are more at risk than others; for instance, a large, well established NGO based in the capital will probably not be as vulnerable as a small, local NGO. We might say that this is common sense, but it can be interesting to analyse why this happens in order to better understand and address the security problems of defenders.

The level of risk facing a group of defenders increases in accordance with threats that have been received and their vulnerability and capacities to those threats, as presented in this equation[1]:

$$\text{RISK} = \frac{\text{THREATS} \times \text{VULNERABILITIES}}{\text{CAPACITIES}}$$

Threats are the possibility that someone will harm somebody else's physical or moral integrity or property through purposeful and often violent action[2]. A threat assessment analyses the likelihood of a threat being put into action.

Defenders can face many different threats in a conflict scenario, including targeting, common crime and indirect threats.

The most common type of threat – targeting - aims to hinder or change a group's work, or to influence the behaviour of the people involved. Targeting is usually closely related to the work done by the defenders in question, as well as to the interests and needs of the people who are opposed to the defenders' work.

Incidental threats arise at least from:

- being in **fighting areas in armed conflicts** ('being in the wrong place at the wrong time').
- **common criminal attacks**, especially if defenders' work brings them to risky areas. Many cases of targeting are carried out under the cover of 'ordinary' criminal incidents.

Targeting (targeted threats) can also be seen in a complementary way: Human rights defenders may come across **direct** (**declared**) threats, for example by receiving a death threat (see Chapter 1.3, for how to assess declared threats). There

A summary of kinds of threats

- Targeting threats (direct /declared) and indirect threats: threats due to your work.
- Threats of common criminal attacks.
- Incidental threats: Threats due to working in armed conflict.

1 Adapted from *Van Brabant* (2000) and REDR.
2 Dworken (1999)

are also cases of **indirect** threats, when a defender close to your work is threatened and there are reasons to believe that you might be threatened next.

Vulnerabilities

Vulnerability is the degree to which people are susceptible to loss, damage, suffering and death in the event of an attack. This varies for each defender or group, and changes with time. Vulnerability is always relative, because all people and groups are vulnerable to some extent. However, everyone has their own level and type of vulnerability, depending on their circumstances. Let's see some examples:

- Vulnerability can be about location: a defender is usually more vulnerable when s/he is out on during a field visit than when s/he is at a well known office where any attack is likely to be witnessed.
- Vulnerability can include lack of access to a phone, to safe ground transportation or to proper locks in the doors of a house. But vulnerability is also related to a lack of networks and shared responses among defenders.
- Vulnerability may also have to do with team work and fear: a defender that receives a threat may feel fear, and his/her work will be affected by fear. If s/he has no a proper way to deal with fear (somebody to talk to, a good team of colleagues, etc) chances are that s/he could makes mistakes or take poor decisions that may lead him/her to more security problems.

(There is a combined check-list of possible vulnerabilities and capacities at the end of this chapter.)

Capacities

Capacities are the strengths and resources a group or defender can access to achieve a reasonable degree of security. Examples of capacities could be training in security or legal issues, a group working together as a team, access to a phone and safe transportation, to good networks of defenders, to a proper strategy for dealing with fear, etc.

In most cases, vulnerabilities and capacities are two sides of the same coin.

For example:

Not knowing enough about your work environment work is a vulnerability, while having this knowledge is a capacity. The same can be said about having or not access to safe transportation or to good networks of defenders.

However, in most cases behaviour is a determining factor

For example:

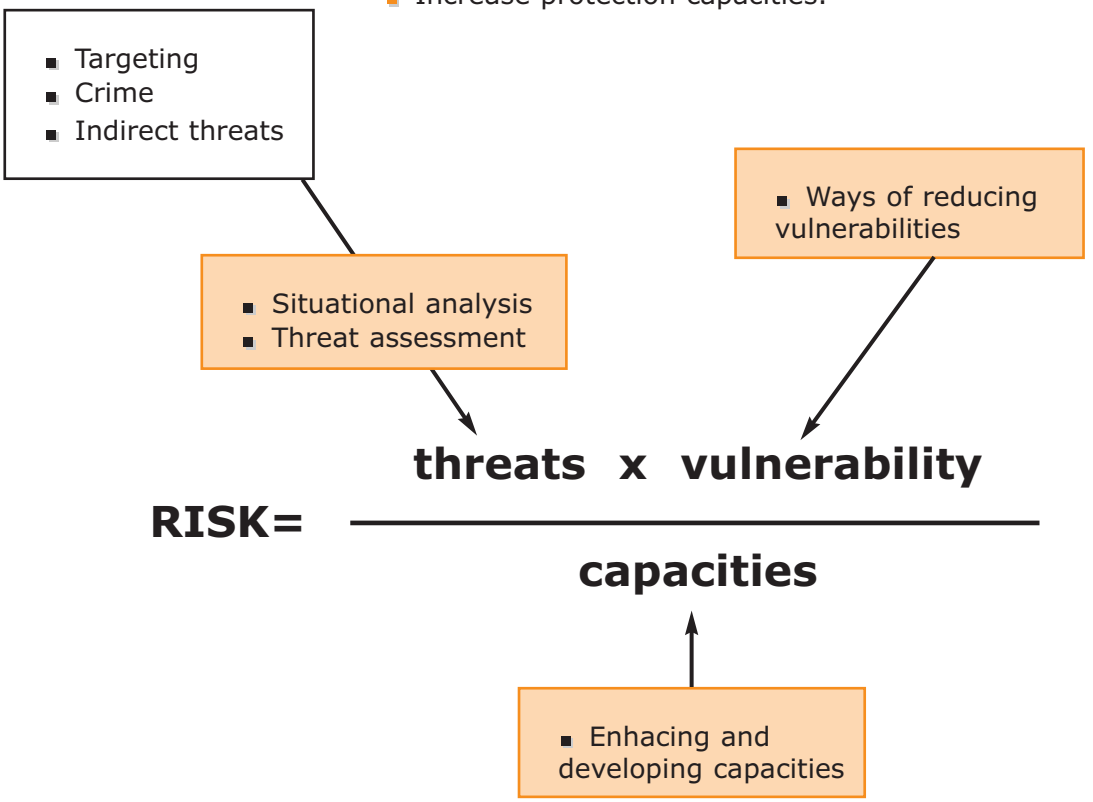
Having a phone can potentially be both a vulnerability and a capacity, depending on how it is going to be used. If it is used loudly and confidential information is communicated, it is a vulnerability. If it used discretely and confidential information is coded, it is a capacity.

(There is a combined check-list of possible vulnerabilities and capacities at the end of this chapter).

In summary,

in order to reduce risk to acceptable levels -namely, to protect- you must:

- Reduce threats.
- Reduce vulnerability factors.
- Increase protection capacities.



Risk is a dynamic concept that changes with time and with variations in the nature of threats, vulnerabilities and capacities. This means risk must be assessed periodically, especially if your working environment, threats or vulnerabilities change. For instance, vulnerabilities can increase if a change of leader-

ship leaves a group of defenders in a weaker position than before. Risk increases dramatically with a clear and present threat. In such cases, it is not safe to try to reduce risk by increasing capacities, because that takes time.

Security measures, such as legal training or protective barriers, can reduce risk by reducing vulnerability factors. However, such measures do not confront the main source of risk, i.e. the threats, nor the will to carry them out, especially in situations where perpetrators know they are likely to go unpunished. All major interventions in protection should therefore aim to reduce threats, in addition to reducing vulnerability and enhancing capacity.

An example:

> *A small group of defenders are working on land property issues in a town. When their work starts affecting the local landowner's interests they receive a clear death threat. If you apply the risk equation to their security situation, you'll see that the risk these defenders face is very high, above all due to the death threat. If you want to reduce that risk it is probably not the moment to start changing the locks on the door of their office (because the risk is not related to a break-in at the office), nor the moment to buy a cell phone for each defender (even if communication might be important to security it is unlikely to be enough if there is someone coming to kill you). In this case, a more relevant strategy would be to work on networking and generating political responses to directly confront the threat (and if that is unlikely to be effective quickly the only way to reduce the risk significantly might be to reduce the defenders exposure, perhaps by moving away for a while – being able to relocate to a safe place is also a capacity).*
> *Making and implementing such a decision also involves a psychosocial capacity for the defender to see that withdrawal is not a synonym of cowardice or defeat… Withdrawing can allow reflection and resuming work once better equipped.*

Vulnerabilities and capacities, as well as some threats, may vary according to gender and age. You therefore need to break down your findings accordingly.

Vulnerabilities and capacities assessment

Designing a vulnerability and capacities assessment for a given group (or person) involves defining the group itself (a community, collective, NGO, individuals, etc), the physical area where it is located and the time line (your vulnerability profile will change and evolve over time). Then you can proceed to assess vulnerabilities and capacities, using the **chart 1.3** at the end of this chapter as guidance.

Please note: The vulnerabilities and capacities assessment must be seen as an open-ended activity aimed at building on existing information to maintain an accurate picture of a constantly evolving situation. When assessing vulnerabilities and capacities, it is important to first draw the current inventory and only then, list the potential and desirable ones. Later, you will need to establish a process to achieve the latter.

Chart 3: Information needed to assess a group's vulnerabilities and capacities.

"Note: Generally speaking, the information in the right column shows vulnerabilities or capacities of each component"

Vulnerabilities and capacities	Information needed to assess the defenders' vulnerabilities or capacities in relation to those components
Components related to geographical, physical and technical features	
Exposure	The need to be in, or to pass through, dangerous areas to carry out normal daily or occasional activities, with threatening actors in those areas.
Physical structures	The characteristics of housing (offices, homes, shelters); building materials, doors, windows, cupboards. Protective barriers. Night lights.
Offices and places open to public	Are your offices open to visitors from the general public? Are there areas reserved only for personnel? Do you have to deal with unknown people that come to your place?
Hiding places, escape routes	Are there any hiding places? How accessible are they (physical distance) and to whom (for specific individuals or the whole group)? Can you leave the area for a while if necessary?
Access to the area	How difficult is it for outside visitors (government officials, NGOs, etc.) to access the area, for example in a dangerous neighbourhood? How difficult is access for threatening actors?
Transport and accommodation	Do defenders have access to safe transportation (public or private)? Do these have particular advantages or disadvantages? Do defenders have access to safe accommodation when travelling?
Communication	Are telecommunications systems in place (radio, telephone)? Do defenders have easy access to them? Do they work properly at all times? Can they be cut by threatening actors before an attack?
Components related to conflict	
Links to conflict parties	Do defenders have links with conflict parties (relatives, from the same area, same interests) that could be unfairly used against the defenders?
Defenders' activities affecting a conflict party	Do defenders' work directly affect an actor's interests? (For example, when protecting valuable natural resources, the right to land, or similar potential targets for powerful actors) Do you work on a specially sensitive issue for powerful actors? (such as land ownership, for example)

Transportation of items and goods and written information	Do defenders have items, goods or information that could be valuable to armed groups, and therefore increase the risk of targeting? (Petrol, humanitarian aid, batteries, human rigths manuals, health manuals, etc.)
Knowledge about fighting and mined areas	Do you have information about the fighting areas that could put you at risk? And about safe areas to help your security? Do you have reliable information about mined areas?
Components related to the legal and political system	
Access to authorities and to a legal system to claim your rights	Can defenders start legal processes to claim their rights? (Access to legal representation, physical presence at trials or meetings, etc.) Can defenders gain appropiate assistance from relevant authorities towards their work and protection needs?
Ability to get results from the legal system and from authorities	Are defenders legally entitled to claim their rights? Or are they subjects to repressive internal laws? Can they gain enough clout to make authorities take note of their claims?
Registration, capacity to keep accounts and legal standards	Are defenders denied legal registration or subjected to long delays? Is their organisation able to keep proper accounts and meet national legal standards? Do you use pirate computer software?
Components related to the management of information	
Sources and accuracy of information	Do defenders have reliable sources of information to base accusations on? Do defenders publicise information with the necessary accuracy and method?
Keeping, sending and receiving information	Can defenders keep information in a safe and reliable place? Could it get stolen? Can it be protected from viruses and hackers? Can you send and receive information safely? Can defenders differentiate top secret and confidential information? Do defenders keep information on them even during non-working time?
Being witnesses or having key information	Are defenders key witnesses to raise charges against a powerful actor? Do defenders have relevant and unique information for a given case or process?
Having coherent and acceptable explanation about your work and aims	Do the defenders have a clear, sustainable and coherent explanation of their work and objectives? Is this explanation acceptable, or at least tolerated, by most/all stakeholders (specially armed ones)? Are all members of the group able to provide this explanation when requested - for example at a checkpoint -?
Components related to social and organisational features	
Existence of a group structure	Is the group structured or organised in any way? Does this structure provide an acceptable level of cohesiveness to the group?

Ability to make joint decisions	Does the group's structure reflect particular interests or represent the whole group (extent of membership)? Are the main responsibilities carried out and decision-making done by only one or a few people? Are back-up systems in place for decision-making and responsibilities? To what degree is decision-making participatory? Does the group's structure allow for: a) joint decision making and implementation, b) discussing issues together, c) sporadic, ineffective meetings, d) none of the above?
Security plans and procedures	Are security rules and procedures in place? Is there a broad understanding and ownership of security procedures? Do people follow the security rules? (For more details, please see Chapter 1.8)
Security management outside of work (family and free time)	How do defenders manage their time outside of work (family and free time)? Alcohol and drug use represent great vulnerabilities. Relationships can also result in vulnerabilities (as well as strengths) How are families and friends involved in the defenders' activities?
Working conditions	Are there proper work contracts for everyone? Is there access to emergency funds? Insurances?
Recruiting people	Do you have proper procedures for recruiting personnel or collaborators or members? Do you have a specific security approach for your occasional volunteers (such as students, for example) or visitors to your organization?
Working with people or with interface organizations	Is your work done directly with people? Do you know these people well? Do you work with an organization as an interface for your work with people?
Taking care of witness or victims we work with	Do we assess the risk of victims and witnesses, etc, when we are working on specific cases? Do we have specific security measures when we meet them or when they come to our office? If they receive threats, how do we react?
Neighbourhood and social surroundings	Are defenders well socially integrated in the local area? Do some social groups see defenders' work as good or harmful? Are defenders surrounded by potentially hostile people (neighbours as informers, for example)? Are supportive neighbours part of the defenders' alarm system?
Mobilization capacity	Are defenders able to mobilize people for public activities?

Components related to psychosocial impact (group/individuals)	
Ability to manage stress and fear	Do key individuals, or the group as a whole, feel confident about their work? Do group/community members clearly express feelings of unity and joint purpose (in both words and action)? Are stress levels undermining good communications and interpersonal relationships? Do people have access to external psychological support and/or have developed internal psychosocial skills?
Deep feelings of pessimism or persecution	Are feelings of depression and loss of hope being clearly expressed (in both words and action)?
Components related to society, culture and religion	
Discrimination	Are defenders discriminated (both outside and inside the organisation) on the basis of gender, ethnicity, religion or different sexual orientation? Is there confusion between human, social, economic, identity, cultural and religious rights?
Components related work resources	
Ability to understand work context and risk	Do defenders have access to accurate information about their working environment, other stakeholders and their interests? Are defenders able to process that information and get an understanding of threats, vulnerabilities and capacities?
Ability to define action plans	Can defenders define and, in particular, implement action plans? Are there previous examples of this?
Ability to obtain advice from well informed sources	Can the group obtain reliable advice? From the right sources? Can the group make independent choices about which sources to use?
People and amount of work	Do the people or personnel available match the amount of work needed? Can you plan field visits in teams (at least two people)?
Financial resources	Do you have enough financial resources for your security? Can you manage cash in a safe way?
Knowledge about languages and areas	Do you know the languages needed for the work in this area? Do you know the area properly? (roads, villages, public phones, health centres, etc.)
Components related to national and international contacts and media	
Access to national and international networks	Do defenders have national and international contacts? To visiting delegations, embassies, other governments, etc? To community leaders, religious leaders, other people of influence? Can you issue urgent actions via other groups? Do you have access to particular organisations or membership status that enhances your protection capacities?
Access to media and ability to obtain results from them	Do defenders have access to media (national, international)? To other media (independent media)? Do defenders know how to manage media relations properly?

A risk scales: Another way to understand risk

A scales provides another way to understand this concept of risk: This is something we migth call ... a "risk-meter". If we put two boxes with our threats and vulnerabilities on one of the plates of the scales, and another box with our capacities on the other plate, we will see how our risk gets increased or reduced:

Fig. 1

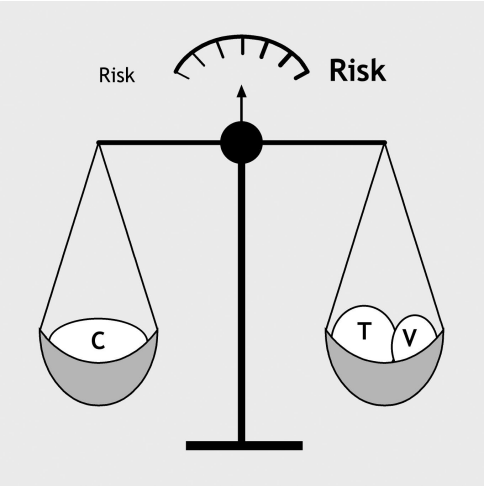
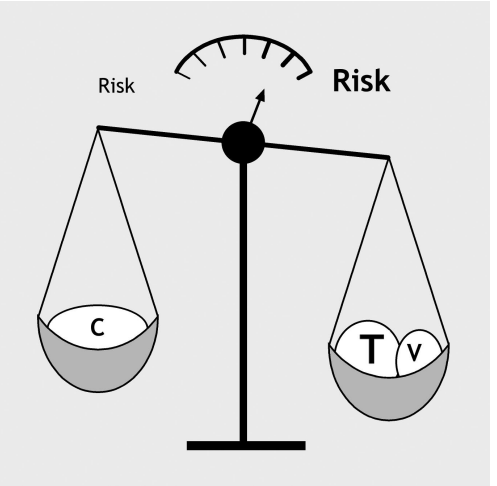
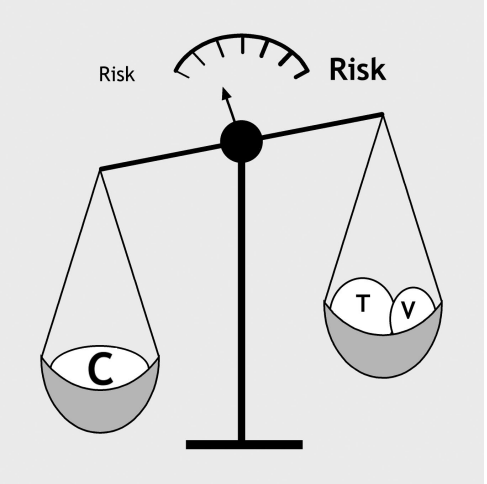


Fig. 2



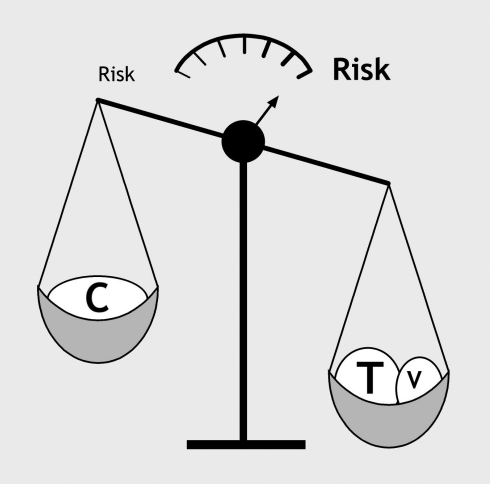
The more threats and vulnerabilities we have, the more risk we face.

Fig. 3



The more capacities we have, the less risk we face. And for reducing the risk, we can reduce our threats and our vulnerabilities, as well as increase our capacities.

Fig. 4



But ... Look at what happens if we have some big threats: Never mind we try to increase our capacities at that very moment: The scales will show a high level of risk anyway!

Summary

$$\text{RISK} = \frac{\text{threats x vulnerability}}{\text{capacities}}$$

Vulnerability and capacities are internal variables (the defenders can work on them)

Threats are external variables (the threats can be made even if they are not feasible)

1 • Working on vulnerability and capacities will result in less feasibility of threats. List the current inventory of your vulnerabilities and capacities. Brainstorming can help.

2 • Separate them per global components and again, per specific components

3 • Set your desirable capacities: work towards them and consider the necessary process to achieve them.

Most of the time, a same set of actions can solve several items of a same component

4 • The result of the above steps will have as impact a reduced feasibility of the threat and therefore a reduced risk

Although some components may be linked to the environment, components can be considered as internal variables on which the defender can work: i.e. a dangerous area is, of course, "external" and yet, the defender can develop the skills ("internal") to deal with it.

A threat is external and whatever is done, the threatener might still threaten. The defender can "only" work on reducing the probability of the threat being put into action and not necessarily on eliminating the threat, unless the political context changes.

CHAPTER 1.3

Understanding and assessing threats

Purpose:

To get an in-depth understanding of threats and how to respond to threats.

Threats assessment: Understanding threats in depth

The repression of human rights defenders is all about psychology. Threats are widely used to make defenders feel vulnerable, anxious, confused and helpless. Ultimately, repression also seeks to break organisations and make defenders lose trust in their leaders and colleagues. Defenders have to tread a fine line between careful and proper management of threats and maintaining a sense of safety in their work. This is also the main objective of this chapter.

In Chapter 1.2, threats were defined as "the possibility that someone will harm somebody else's physical or moral integrity or property, through purposeful, often violent action". We also talked about **probable (indirect)** threats (when a defender close to your work is threatened and there is reason to believe you might be threatened next), and **declared (direct)** threats (receiving a death threat, for example). We will now look at how to deal with **declared threats**.

A declared threat is **a declaration or indication of an intention to inflict damage, punish or hurt, usually in order to achieve something**. Human rights defenders receive threats because of the impact their work is having, and most threats have a clear objective to either stop what the defender is doing or to force him or her to do something.

A threat always has a **source**, i.e. the person or group who has been affected by the defender's work and articulates the threat. A threat also has an **objective** which is linked to the impact of the defender's work, and a **means of expression**, i.e. how it becomes known to the defender.

Threats are tricky. We might say with a certain amount of irony that threats are "ecological", because they aim to achieve major results with a minimum investment of energy. A person making a threat has chosen to do that, rather than take action - a higher investment of energy. Why? There may be a number of reasons why, and it is worth mentioning them here:

- The person making the threat has the capacity to act but is to some extent concerned about the political cost of acting openly against a human rights defender. Anonymous threats can be issued for the same reason.
- The person making the threat has a limited capacity to act and intends to achieve the same aim by hiding his or her lack of capacity behind a threat. This limited capacity may only be temporary due to other priorities, or permanent, but in both cases things may change and lead to direct action against the defender later on.

A threat is a personal experience. Threats always affect people in some way. One defender once said that: "Threats achieve some effect, even only due to the fact that we are talking about threats". In fact, any threat can have a double impact: emotionally, and in terms of security. We will concentrate on security here, but we should not forget the emotional side of every threat or the impact of emotions on security.

We know that a threat is usually linked to the impact of our work. Receiving a threat therefore represents feedback on how your work is affecting someone else. If you look at it in this way, a threat is an invaluable source of information, and should be analysed carefully.

"Making" vs. "posing" a threat

People issue threats against human rights defenders for many reasons, and only some have the intention or capacity to commit a violent act. However, some individuals can represent a serious threat without ever articulating it. This distinction between *making* and *posing* a threat is important:

- Some people who **make** threats ultimately **pose** a threat;
- Many people who **make** threats **do not pose** a threat;
- Some people who **never make** threats **do pose** a threat.

A threat is only credible if it suggests that the person behind it has the capacity to act against you. It has to demonstrate a minimum level of force or have a menacing element designed to provoke fear.

The person behind the threat can demonstrate his or her capacity to act quite simply, for example by leaving a written threat inside a locked car, even when you have left it parked for just a few minutes, or by phoning just after you have arrived home, letting you know you are being watched.

People can try to instil fear in you by introducing symbolic elements into threats, for example by sending you an invitation to your own funeral or putting a dead animal on your doorstep or on your bed at home.

Many threats show a combination of the above characteristics. It is important to distinguish between them, because some people who send threats pretend to have the capacity to act by using symbolic and frightening elements.

Anyone can make a threat, but not everyone can pose a threat.

At the end of the day, you need to know whether the threat can be put into action. If you are reasonably sure that this is unlikely, your approach will be completely different than if you think a threat has some basis in reality.

The three main objectives when assessing a threat are:

- To get as much information as possible about the purpose and source of the threat (both will be linked to the impact of your work);
- To reach a reasoned and reasonable conclusion about whether the threat will be acted on or not.
- To decide what to do

Five steps to assessing a threat

1 • **Establish the facts surrounding the threat(s).** It's important to know exactly what has happened. This can be done through interviews or by asking questions to key people, and occasionally through relevant reports.

2 • **Establish whether there is a pattern of threats over time.** If several threats are made in a row (as often happens) it is important to look for patterns, such as the means used to threaten, the times when threats appear, symbols, information passed on in writing or verbally, etc. It is not always possible to establish such patterns, but they are important for making a proper threat assessment.

3 • **Establish the objective of the threat.** As a threat usually has a clear objective linked to the impact of your work, following the thread of this impact may help you establish what the threat is intended to achieve.

4 • **Establish the source of the threat.** (This can only be done by going through the first three steps first.) Try to be as specific as possible and distinguish between the principal and agent: for example, you could say that "the government" is threatening you. But since any government is a complex actor, it is more useful to find out which part of the government may be behind the threats. Actors such as "security forces" and "guerrilla groups" are also complex actors. Remember that even a signed threat could be false. This can be a useful way for the person making the threats to avoid political costs and still achieve the aim of provoking fear in a defender and trying to prevent him or her from working.

5 • **Make a reasoned and reasonable conclusion about whether or not the threat can be put into action.** Violence is conditional. You can never be completely sure that a threat will – or will never - be carried out. Making predictions about violence is about stating that, given certain circumstances, a specific risk exists that a particular person or group will act violently against a particular target.

Defenders are not fortune- tellers and cannot pretend to know what is going to happen. However, you can come to a reasonable conclusion about whether or not a given threat is likely to be put into action. You may not have gained enough information about the threat through the previous four steps and may therefore not reach a conclusion. You may also have different opinions about how "real" the threat is. In any case, you have to proceed on the basis of the worst case scenario.

For example:

> *Death threats have been made against a human rights worker. The group analyse the threats and reach two opposing conclusions, both based on good reasoning. Some say the threat is a total fake, while others see worrying signals about its feasibility. At the end of the meeting, the group decides to assume the worst case scenario, i.e. that the threat is feasible, and take security measures accordingly.*

This threat assessment progresses from solid facts (step 1) to increasingly speculative reasoning. Step 2 involves some interpretation of the facts, and this increases further through steps 3 to 5. There are good reasons for following the order of the steps. Going directly to step 2 or 4, for example, will miss out the more solid information arising from the previous steps.

Maintaining and closing a threat case

A threat or security incident can alarm a group of defenders, but it is usually difficult to maintain this perception of alarm for as long as the threat lasts. Because of the constant outside pressure on defenders in their work, ringing organisational alarm bells too often could lead the group to lose interest and come off their guard.

Raising a group alarm should only happen based on reliable evidence and should be focused on a specific anticipated event. It must be designed to motivate group members to act, and call for a specific set of actions to be taken. To be most effective, an alarm should only stimulate a moderate level of motivation: too low doesn't get people to act, but too high creates emotional overload. If the threat is likely to persist over time, it is essential to debrief people and do follow-up after the initial alarm was raised to correct misinformation, change misguided recommendations, and reinforce the group's trust in their joint efforts.

Finally, if the threat does not materialise, some explanation of why must be provided, and the group should be informed that the threat is lower or has disappeared altogether.

You can consider closing a threat case when the potential attacker is deemed to no longer pose a threat. Ideally, to be sure that you are right to close a case, you should be able to explain why first. Questions should also be asked about changed circumstances which could trigger the person behind the threats to move towards violent action.

Reacting to threats in security terms

- A threat can be considered a security incident. To find out more about responding to security incidents, turn to Chapter 1.4.
- An assessment of declared threats can lead you to think that you could be attacked. Please see Chapter 1.5, on preventing attacks.

Summary

Threats can be incidental, direct (declared) and indirect (not declared).

A declared threat is a declaration or indication of intention against someone to achieve something.

Five steps will help establish the feasibility of the threat in order to take a decision about what to do:

1. Establish the facts
2. Establish the pattern over time
3. Establish the objective
4. Establish the source
5. Draw a reasoned and reasonable conclusion about the feasibility of the threat.

Avoid instant "obvious" conclusions and try to be as specific as possible by opening as many scenarios as facts and patterns indicate and by developing them as far as you can substantiate them.

CHAPTER 1.4

Security incidents: definition and analysis

Purpose:

Learning how to recognise and respond to security incidents.

What is a security incident?

Put simply, a security incident can be defined as **any fact or event which you think could affect your personal or organizational security.**

Security incidents can be incidental or provoked intentionally or unintentionally.

Examples of security incidents could include seeing the same, suspicious vehicle parked outside your office or home over a number of days; the telephone ringing at night with nobody at the other end; somebody asking questions about you in a nearby town or village, a break-in to your house, etc.

But not everything you notice will constitute a security incident. You should therefore **register** it, by writing it down, and then **analyse** it, ideally with colleagues, to establish if it really could affect your security. At this point you can **react** to the incident. The sequence of events is as follows:

> You notice something ⇨ you realise it might be a security incident ⇨ you register it / share it ⇨ you analyse it ⇨ you establish that it is a security incident ⇨ you react appropriately.

If the matter is pressing, this sequence should still take place, just much more quickly than usual to avoid delay (see below).

How to distinguish between security incidents and threats:

If you are waiting for a bus and somebody standing next to you threatens you because of your work, this - apart from being a threat - constitutes a security incident. But if you discover that your office is being watched by a police car from the opposite side of the street, or your mobile phone is stolen, these are security incidents, but not necessarily threats. However, while incidental and unintentionally provoked security incidents can clearly be distinguished from the threats, remember that intentionally provoked security incidents have got an objective

and not necessarily the same as threats (see Chapter 1.2). The minimum objective of an intentionally provoked incident is to gather information about the defenders regardless if it is going to be used against them.

Establishing a clear distinction is important at least for the mental health of the defenders.

All threats are security incidents, but not all security incidents are threats.

Why are security incidents so important?

Security incidents are crucial in handling your security because **they provide vital information about the impact your work is having, and about possible action which may be planned or carried out against you.** Likewise, such incidents allow you to change your behaviour or activities and avoid places which could be dangerous, or more dangerous than normal. Security incidents can therefore be seen as indicators of the local security situation. If you couldn't detect such changes it would be difficult to take appropriate and timely action to stay safe.

For instance, you may realize that you are under surveillance after noticing several security incidents: now you can take action about surveillance.

Security incidents represent "the minimum unit" of security measurement and indicates the resistance/pressure on your work. Do not let them go unnoticed!

When and how do you notice security incidents?

This depends on how obvious the incident is. If it could potentially go unnoticed, your ability to recognise it depends on your security training and experience and your level of awareness.

The greater your awareness and training, the fewer incidents will escape your attention.

Security incidents are sometimes overlooked or briefly noticed and then brushed to one side, or people sometimes overreact to what they perceive as security incidents.

Why might a security incident go unnoticed?

An example:

A defender experiences a security incident, but the organisation s/he works with does not react at all. This could be because…

- the defender isn't aware that a security incident took place
- the defender is aware of it but dismisses it as unimportant

- the defender hasn't informed the organisation (s/he forgot, doesn't believe it necessary, or decide to keep quiet because it happened because of a mistake on their part)
- the organisation, having done a team evaluation of the incident after the defender registered it in the incident book, does not judge action necessary

Why do people sometimes overreact to security incidents?

For example:

A colleague might be constantly telling stories about some security incident or other, but on further examination they prove not to have substance or merit the definition. The actual security incident in this instance is the fact that your colleague has a problem which makes him/her see non-existent security incidents. S/he might be feeling very afraid, or suffering from stress, and should be offered support to resolve the problem.

Do not forget that that security incidents are overlooked or dismissed to often: be careful about this!

Dealing with security incidents

You can deal with security incidents in three basic steps:

1 • **Register them.** All security incidents noticed by a defender must be registered, either in a simple, personal notebook or one accessible to the whole group.

2 • **Analyse them.** All registered security incidents should be properly analysed straight away or on a regular basis. It is better to analyse them as a team rather than individually because this minimises the risk of missing something. Someone should be put in charge of making sure this is done.

Decisions must also be made about whether or not to maintain confidentiality about specific incidents (such as threats). Is it ethical and realistic to keep a threat hidden from colleagues and other people you work with? No single rule applies to every situation, but it is often best to be as open as possible in terms of sharing information and addressing logistical concerns, as well as fears.

3 • **React to them.** Given that security incidents give feedback on the impact of your work, they could lead to the following:

- Reaction to the incident itself;
- **Feedback**, in security terms, about how you work, your work **plans** or your work **strategy**. **For example:**

Example

of an incident which provides **feedback** on working more securely:

For the third time somebody from your organisation has had problems passing through a police checkpoint because they frequently forget to carry the necessary documents. You therefore decide to compile a checklist which all staff members must consult before leaving the city. You might also change the route for these types of journeys.

Example

of an incident which providing feedback on how you **plan** for security:

At the same police checkpoint, you are detained for half an hour and told that your work is poorly regarded. Thinly veiled threats are made. When you ask for an explanation at police headquarters, the scene is repeated. You call a team meeting to revise your work plans, because it seems clear that changes have to be made in order to continue working. You then plan a series of meetings with Interior Ministry civil servants so that checkpoint police is instructed to refrain from harassing you, change some aspects of your plans and arrange weekly meetings to monitor the situation.

Example

of an incident which provides feedback for your security **strategy**:

When you start work as defenders in a new area, you immediately receive death threats and one of your colleagues is physically assaulted. You did not anticipate such opposition to your work, nor provide for it in your global strategy. You will therefore have to change your strategy in order to develop tolerance of your work locally and deter further attacks and threats. To do this you may have to suspend your work for a while, withdraw from the area and reconsider the entire project.

Reacting *urgently* to a security incident

There are many ways of responding promptly to a security incident. The following steps have been formulated in terms of when and how to react from the moment a security incident is reported, while it is happening, and after it is over.

Step 1: Reporting the incident.

- What is happening/has happened (try to focus on the actual facts)?
- Where and when did it take place?
- Who was involved (if it can be established)?
- Was there any injury or damage to individuals or property?

Step 2. Decide when to react. There are three possibilities:

- An **immediate reaction** is required to attend to people with injuries or stop an attack.
- A **rapid reaction** (in the next few hours or even days) is necessary to prevent possible new security incidents from arising (the incident is over).
- A **follow up action** (in several days, weeks or even months): if the situation has stabilised, an immediate or rapid reaction may not be necessary. However, any security incident that requires an immediate or rapid reaction must be followed by a follow-up action in order to restore or review your working environment.

Step 3. Decide how to react and what your objectives are.

- If the reaction has to be immediate, the objectives are clear: attend to injuries and/or prevent another attack.
- If the reaction has to be quick, the objectives will be established by the person in charge or a crisis team (or similar) and **focus on restoring the necessary security for those affected by the incident.**

Subsequent actions/reactions will take place through the organisation's normal decision-making channels, with the objective of restoring a safe working environment externally, as well as re-establishing internal organisational procedures and improving subsequent reactions to security incidents.

Any reaction also has to take into account the security and protection of other people or organisations or institutions with which you have a working relationship.

**Establish your objectives before taking action.
Prompt action is important, but knowing why you are taking action is more important. By first establishing what you want to achieve (objectives), you can decide how to achieve it (course of action).**

For instance:

If a defenders' group receives news that one of their colleagues has not arrived at her destination in a town, they may start a reaction by calling a hospital and calling their contacts in other NGOs and a nearby UN Office and police. But before starting those calls, it is very important to establish what you want to achieve and what you are going to say. Otherwise you may generate unnecessary alarm (imagine that the defender was just delayed because they missed a bus and forgot to call the office) or a reaction opposite to the one intended.

Summary

A security incident is any fact or event which you think could affect your personal or organizational security.

Security incidents can be incidental or provoked intentionally or unintentionally.

Security incidents measure security and the impact of defenders' work on others' interests.

All defenders have security incidents. The contrary would imply that:

- The impact of the defenders' work is insignificant either because the work is not carried out properly and/or because nobody's interest is being affected. In other words: no one is interested in them.
- The potential aggressor has already got all information about the defenders and doesn't need to bother: the defenders were not able to spot the provoked security incidents then

A security incident is not a threat, however it needs attention.

Three steps to deal with security incidents:

1 • Register them

2 • Analyse them

3 • React to them

Preventing and reacting to aggressions

Purpose:

Assessing the likelihood of different kinds of aggression taking place.

Preventing possible direct aggression against defenders.

Carrying out counter - surveillance.

Aggressions against human rights defenders

Violence is a process, as well as an act. A violent aggression against a defender does not take place in a vacuum. Careful analysis of aggressions often shows that they are the culmination of conflicts, disputes, threats, security incidents and mistakes which can be traced over time.

Aggressions against defenders are the product of at least three interacting factors:

1 • **The party who takes the violent action.** Aggressions on defenders are often the product of processes of thought and behaviour we can understand and learn from even if they are illegitimate.

2 • **Background and triggers which lead the aggressor to see violence as an option.** Most people who aggress defenders see aggressing as an "useful" way of reaching a goal or "solving a problem".

3 • **A setting** that facilitates violence, allows it to take place or does not stop it.

Who, then, is a danger to defenders?

Generally, anyone who thinks that aggressing a defender is a desirable, acceptable, or potentially effective way to achieve a goal can be considered a potential aggressor. The threat increases if s/he also has, or can develop, the capacity to aggress a defender.

The threat of an aggression can decrease with changes in the potential aggressor's capacity to stage an aggression, their attitude towards how acceptable an aggression is, or how likely s/he is to be caught and punished.

Some aggressions are preceded by threats. Others are not. However, the behaviour of individuals planning a targeted violent aggression often shows subtle signs, since they need to gather information about the right time to aggress, plan how to get to their target, and how to escape.

It is therefore vital to detect and analyse any signs indicating a possible aggression. This involves:

- Determining the likelihood of a threat being carried out (see Chapter 1.3);
- Identifying and analysing security incidents.

Security incidents which involve surveillance of defenders or their workplace are aimed at gathering information. This information isn't always intended for use in an aggression, but it is important to try and establish whether it is or not (see Chapter 1.4). Surveillance can be used for a number of purposes:

- To establish what activities are carried out, when and with/by whom.
- To use this information later to aggress individuals or organisations.
- To gather the information necessary to carry out an aggression.
- To gather information for legal action or other harassment (without direct violence).
- To intimidate you, your supporters or other people who work with you.

It is important to remember that surveillance is usually necessary in order to carry out an aggression, but doesn't in itself constitute an aggression. Also, not all surveillance is followed by an aggression. Targeted violence does sometimes occur in situations when an aggressor suddenly sees an opportunity to strike, but even then some level of preparation has usually been carried out first.

There is little information available to help you recognise an aggression being prepared. The absence of studies on this subject contrasts sharply with the large number of aggressions against defenders. However, the studies which do exist offer some interesting insights [1].

- **Aggressing a defender isn't easy and requires resources.** Surveillance is needed to establish an individual's movements and the best

[1] Claudia Samayoa and Jose Cruz (Guatemala) and Jaime Prieto (Colombia) have produced interesting studies on aggressions against human rights defenders. Mahony and Eguren (1997) also carried out an analysis of such aggressions.

location for aggressing. Getting to the target and making an effective, quick escape is also vital. (However, if the environment is highly favourable to the aggressor, aggressions are easier to carry out.)

- **People who aggress defenders usually show a degree of consistency.** The majority of aggressions are aimed at defenders who are heavily involved in issues affecting the aggressors. In other words, aggressions are not usually random or aimless, but respond to the interests of the aggressors.

- **Geographical factors matter.** For example, aggressions on defenders in rural areas may be less public and therefore provoke less reaction at law enforcement level and political level than aggressions in urban areas. Aggressions against NGO headquarters or high profile organisations in urban areas generate a greater reaction.

- **Choices and decisions are made before an aggression.** People who are considering an aggression against a defenders' organisation must decide whether to aggress the leaders or grassroots members, and choose between a single hit (against a key, possibly high- profile person and therefore at an increased political cost for the agressor) or a series of aggressions (affecting the organisation's membership). The few studies done on aggressions against defenders suggest that both strategies are usually applied.

Establishing the feasibility of an aggression

To find out how likely an aggression is, you need to analyse the factors involved. To establish what those factors are, it is useful to differentiate between different kinds of aggressions, i.e. common crime, incidental aggressions (being in the wrong place at the wrong time) and direct aggressions (targeting), using the three tables on the following pages [2].

[2] This classification of aggressions includes the same categories as for threats: Please have a look at the chapter on threats for clarification.

Table 1: Establishing the probability of direct aggressions (targeting)

(**PA** stands for potential aggressors)

Probability of direct aggressions (Targeting)			
Factors	Low Probability	Medium Probability	High Probability
Capacity to aggress	PA have limited ability to act in the areas where you work	PA have operational capacity near the areas where you work	Zones where you work are under the firm control of PA
Financial motive	PA do not need your equipment or cash for their activities	Interest in your equipment, cash, or other forms of financial gain (i.e. kidnapping)	PA in clear need of equipment or cash
Political and military motive	None - your work has nothing to do with their objectives	Partial interest - your work limits their political and military objectives	Your work clearly hampers their objectives, benefits their opponents, etc.
Record of previous aggressions	None or rare	Occasional cases	Many previous cases
Attitudes or intentions	Sympathetic or indifferent attitude	Indifferent Occasional threats Frequent warnings	Aggressive, with clear and present threats
Security forces' capacity to deter aggressions	Existing	Low	None, or security forces collaborate with (or become) PA
Your level of political clout against PA	Good	Medium to low	Limited (depending on circumstances) or none

Example

of the probability of direct aggressions (targeting):

The PA control the areas in which you work, but they do not have any financial motive for aggressing you. Your work only partially limits their political and military objectives, and there are no precedents of similar aggressions in the city. Their attitude is indifferent, and they do clearly not want to attract any national or international attention or pressure by aggressing you.

The probability of direct aggressions in this scenario is considered to be low to medium.

Table 2: Establishing the probability of crime aggression

(**CO** stands for criminal offenders)

Probability of crime aggression			
Factors	Low Probability	Medium Probability	High Probability
Mobility and location of CO	CO usually stay in their own areas, away from your zones	CO generally enter other areas at night (or operate close to your work areas)	CO operate anywhere, day or night
Aggressiveness of CO	CO avoid confrontation (predominantly commit crime where you do not stay usually)	CO commit crime in the street (but not in staffed offices)	CO openly commit street robberies and enter premises to commit crime
Acces to/use of weapons	Unarmed or use non-lethal arms	Crude weapons, including machetes	Firearms, sometimes powerful
Size and organisation	Operate individually or in pairs	2-4 people operate together	Operate in groups
Police response and deterrence	Rapid response, capable of deterrence	Slow response, little success capturing criminals in the act	Police do not usually respond with even a minimum degree of effectiveness
Training and professionalism of security forces	Well trained and professional (it maybe that they lack resources)	Regular training, low pay, limited resources	Police are either non-existent or corrupt (cooperate with offenders)
General security situation	There is lawlessness but the situation is relatively secure	Lack of security	Rights not observed, absolute impunity

Example

of an assessment of probability of crime aggression:

*In this city, criminals operate in different areas in pairs or small groups, sometimes during the day. They are often aggressive and often carry guns. The police does respond, but slowly and ineffectively, and the police force is unprofessional and under-resourced. However, the police leadership is well disciplined. There is a clear lack of security, and if applied to the marginal neighbourhoods of the city, the probability of crime aggression is at its highest given that **all** the indicators are at high level.*

The probability of a criminal aggression in the centre of a city like this is at a high to medium level

Table 3: Establishing the probability for incidental aggressions

(**PA** stands for potential aggressors)

Probability of incidental aggressions			
Factors	Low Chance	Medium Probability	High Probability
Your knowledge of conflict areas	Good	Approximate	You know very little about where combat zones are located
Distance to conflict areas	Your work is far away from these areas	Your work is close to these areas and you occasionally enter them	Your work is carried out in combat zones
Movement of conflict areas	Conflicts zones are static, or change slowly and verifiably	They change relatively often	They change continually, making them unpredictable
Your knowledge of location of areas with landmines	You have good knowledge or there are no mined areas	Approximate knowledge	Unknown
Distance between your work place and areas with landmines	Your work takes place far away from these areas, or there are none	Your work is close to these areas	Your work takes place among mined areas
Combat tactics and arms	Discriminate	Discriminate, with occasional use of artillery, ambushes and snipers	Indiscriminate: bombardment, heavy artillery, terrorist or bomb attacks

Example

of an assessment of probability of incidental aggressions:

In this area, you are familiar with the combat zones, which change slowly and verifiably. Your work is close to the areas where the fighting takes place and you occasionally visit or stay in the combat zones. You are not close to mined areas. The combat tactics used are discriminate and therefore do not affect civilians very often.

Work in this zone carries a low level of risk of incidental aggression.

Preventing a possible direct/indirect aggressions

Although the defender is the target in both cases, let's distinguish between:

- direct aggression against the defender
- indirect aggression against the defender when it involves someone close to the defender

In both cases prevention will require the same underlying logic.

You now know that a threat can decrease with changes in the potential aggressor's capacity to stage an aggression, their attitude towards how acceptable an aggression is, or how likely s/he is to be caught and punished.

To prevent an aggression it is therefore necessary to:

- Persuade a potential aggressor or a person making threats that an aggression will involve unacceptable costs and consequences;

- Make aggression less feasible.

This type of aggression prevention is parallel to the analysis covered in Chapter 1.2, which states that risk is dependent on the defenders' vulnerabilities and capacities. In order to protect yourselves and reduce risk, you need to take action against the threat, reduce your vulnerabilities and enhance your capacities.

When a threat is made and you want to reduce the risk associated with it, it is important to act - not just against the threat itself, but also on the **vulnerabilities** and **capacities** most closely related to the threat. At times of great pressure, when you want to react as quickly as possible, you often act on the vulnerabilities which are easiest to deal with or closest to hand instead of those which are most relevant to the threat.

Be careful: If the risk of aggression is high (that is, if the threat is strong and real, and there are several vulnerabilities and fewer capacities), working on vulnerabilities or capacities to reduce the risk makes little sense, because these require time to change and become functional. If the risk is very high (a direct and severe aggression is imminent) you can only do three things to avoid it:

a ◆ Immediately and effectively confront the threat, knowing that you can achieve an immediate and specific result which will prevent the aggression. (Usually it is very difficult to be sure that there will be an immediate and effective result, because reactions take time, and time is precious in this situation.)

b ◆ Reduce your exposure to as close to zero as possible, by going into hiding or leaving the area [3].

[3] However, there will be occasions where attempting to travel might put someone at greater risk.

c ◆ Seek effective protection!: see two examples of what might be effective protection (depending on context):

- Community protection: if you hide or seek refuge in a community, public eye and witnesses might deter the potential aggressor.

- Armed protection: it might be somehow useful in a few cases, but assuming that it is close at hand (immediate), that it can deter the potential aggressor and that it does not put the defender in more danger in the medium or long term. Realistically, such requirements of armed protection are very difficult to fulfil! Some Governments offer armed escorts to defenders, after national or international pressure; in these cases, accepting or rejecting the escort may have to do with holding the state accountable for the security of defenders, but a Government can never say that it is relieved of its responsibilities if the defender does not accept the armed escorts. Private security companies may lead to more risk if they are linked to aggressors[4] And for defenders, to carry weapons, we must say, is usually ineffective against an organized aggression, and may also make defenders vulnerable if a Government uses this as a pretext for attacking them on the basis of fighting terrorism or insurgency. Moreover, carrying weapons could be twisted against the defender as being in contradiction with the UN declaration on HRD.

Threatening situations that can lead to an aggression are easier to handle if other relevant actors or stakeholders become involved and work together. Examples include a functioning judicial system, support networks (domestic and international) that can put political pressure on duty-bearer stakeholders, social networks (within or among organisations), personal and family networks, UN/international peacekeepers, etc.

Surveillance and counter-surveillance

Counter-surveillance can help you establish whether you are being watched. It is difficult to find out whether your communications are being intercepted, and for this reason you should always assume that they are[5]. However, it is possible to determine if your movements and offices are being watched.

Who could be watching you?

People who are usually in your area, such as doormen or porters in buildings, travelling sales people who work close to the building entrance, people in nearby vehicles, visitors, etc, could potentially all be watching your movements. People do surveillance for money; because they are being pressurised to do it; because of their sympathies, or due to a combination of these factors. Those behind the surveillance may also place collaborators or members of their organisation in your area.

4 For more information please see in this Manual the chapter on "Improving security at work and home".

5 For more information see in this Manual the chapter on securing communications.

People can also watch you from a distance. In this case they are almost always members of an organisation and will probably use the tactic of watching without wishing to be seen. This means keeping a certain distance, various people taking turns and watching from different locations, using different vehicles, etc.

How to know if you are being watched

You can find out if you're being observed by watching those who could be watchingyou and by adopting the following rules (without, of course, becoming paranoid):

- If you have reason to think that somebody might want to watch you, you should be mindful of the movements of people in your area and changes in their attitude, for example, if they start asking about your activities. Remember that both women and men can carry out surveillance, as can old or very young people.

- If you suspect that you are being followed, it is possible to put in place a counter-surveillance measure involving a third party whom you trust, and who is unknown to those who might be watching you. This third party can watch, in advance and from a good distance, movements which occur when you arrive, leave or go somewhere. Whoever is watching will probably do so from a place where you can always be easily located, including your home, offices and the places where you most often do your work.

For example

Before arriving home you can ask a family member or trusted neighbour to take up a position close by (e.g., changing a car wheel), to check if somebody is awaiting your arrival. The same can be done when leaving your office on foot. If you are using a private vehicle, it will be necessary to have another car leave after yours in order to allow a potential observer time to begin their approach towards you.

The benefit of counter-surveillance is that, at least initially, the person observing you does not realise you know they are there. It should therefore be made clear to anyone involved in the counter-surveillance that it may not be advisable to confront the person observing you. They will then realise that you know about their activities, and this could also provoke a violent reaction. It is important to take the utmost care and keep a distance if you are aware of somebody watching you. Once surveillance has been detected, you can take the action recommended in this manual[6] .

Most of this counter-surveillance advice applies almost exclusively to urban and semi-urban areas. In rural areas the situation is very different, but defenders and communities who live in such areas are more used to being aware of strangers nearby. It is therefore more difficult for somebody who wants to watch you to gain access to inhabitants of a rural area - unless the local population is deeply hostile towards your work.

6 See chapter on "Improving security at work and home"

Note: building a relationship with the security forces monitoring you could be beneficial in some circumstances. In some circumstances the surveillance will not be a secret as part of the point is to make it visible/intimidating. In some situations defenders cultivate people in the security forces who can sometimes tip them off when surveillance or even an action is planned against them

When to check if you are being watched.

Logic dictates that it is wise to check if you are under surveillance if you have reason to believe that you are - for example, because of security incidents which could be related to surveillance. If your human rights work carries a certain risk, it is a good idea to conduct a simple counter-surveillance exercise from time to time, just in case.

You need also to think about risk you bring to others if you are under surveillance – the risk may be greater for a witness/family member of a victim you are meeting than for you. Think about where would be most secure for them to meet. You may need to warn them that your movements might be under surveillance.

Reacting to aggressions

No single rule can be applied to all aggressions against defenders. Aggressions are also security incidents, and you can find guidelines for how to react to security incidents in Chapter 1.4.

In any kind of aggression there are two essential things to remember:

- Think always about security! Both during and **after** the aggression. (If you are under aggression and you have to make a choice between two alternatives, go for the safest one!)

- Following an aggression, it will be necessary to recover physically and psychologically, take action to solve the situation, and restore a safe work environment for you and your organisation. It is crucial to retain as much detailed information as possible about the aggression: what happened, who/how many people were involved, number plates of vehicles, descriptions, etc. This can be useful to document the case, and should be compiled as quickly as possible. Keep copies of any documents handed over to the authorities to document the case.

Summary

Aggression is the culmination of a process which definitely included security incidents, maybe threats.

Thus aggression is not an "unexpected" event.

Aggression can be incidental or targeted

It is not easy to aggress human rights defenders as they are public figures and enjoy some kind of support.

Aggression is the product of 3 interacting factors:

- The party who takes the violent action
- Background and triggers which lead the aggressor to see violence as an option
- A suitable setting

An aggression requires adequate resources and capacities, access to the individual, a quick escape and a certain level of impunity or the decision by the aggressor that it is worth the political cost.

Therefore, preventing an attack requires actions both to maintain the political cost as high as possible (reduce impunity level) and to reduce one's physical exposure to risk as close as possible to zero.

CHAPTER 1.6

Drawing a global security strategy

Purpose:

Recognizing strategies and tactics already in place

Analysing strategies and tactics already in place

Defining the global strategy to occupy work space

Ad hoc deterrence strategy and tactics

Defenders and groups under threat use different ad hoc deterrence strategies to deal with perceived risks. These strategies will vary a lot depending on their environment (rural, urban), the type of threat, the social, financial and legal resources available, etc.

Most ad hoc strategies can be implemented immediately and in response to short- term objectives. They will therefore function more like tactics than as global response strategies. Most strategies also respond to individual people's subjective perceptions of risk, and could at times cause the group some level of harm, especially if the strategies used cannot be reversed.

Ad hoc strategies are closely related to the type and severity of threat and to the group's capacities and vulnerabilities.

When thinking about security and protection you must take into account both your own and other people's ad hoc strategies. Reinforce the effective ones, try to limit harmful ones and try to respect the remaining ones (especially ad hoc strategies linked to cultural or religious beliefs).

Some ad hoc strategies:

- Reinforcing protective barriers, hiding valuables.
- Avoiding behaviour which could be questioned by another actor, especially if control of the territory where you are working is under military dispute.
- Going into hiding during high risk situations, including in places that are difficult to access, like mountains or jungle, changing houses, etc. Sometimes

whole families go into hiding, and sometimes just defenders. Hiding could take place at night or go on for several weeks, and might involve no outside contact.

- Looking for armed or political protection from one of the armed actors.
- Suspending activities, closing down the office, evacuating. Forced migration (internal displacement or as refugees) or going into exile.
- Relying on "good luck" or resorting to religious and "magic" beliefs.
- Becoming more secretive, including with colleagues; going into denial by refusing to discuss threats; excessive drinking, overwork, erratic behaviour.

Defenders also have access to response strategies. These can include issuing reports to publicise a specific issue, making allegations, staging demonstrations, etc. In many cases these strategies do not amount to a long term strategy, but respond to short term needs. In some cases the response strategies might even create more security problems than those they were intended to address.

Analysing deterrence strategy

Whether global or ad hoc deterrence strategy, take the following into account:

- **Responsiveness:** Can your strategies respond quickly to individual or group security needs?
- **Adaptability:** Can your strategies be quickly adapted to new circumstances, once the risk of attack is over? A defender may have several options available, for example to either hide or to live at other people's houses for a while. Such strategies may seem weak or unstable, but often have great endurance.
- **Sustainability:** Can your strategies endure over time, despite threats or non-lethal attacks?
- **Effectiveness:** Can your strategies adequately protect the people or groups in question?
- **Reversibility:** If your strategies don't work or the situation changes, can your strategies be reversed and/or changed?

Dealing with risk after doing a risk assessment

Once your risk assessment has been done, you need to look at the results. As it is impossible to measure the "amount" of risk you are facing, you need to establish an understanding of what the **level** of risk is.

Different defenders and organisations may perceive different levels of risk. What is unacceptable for some defenders can be acceptable for others, even within the

same organisation. Rather than discussing what "must" be done or whether you are prepared for going ahead with it, people's different thresholds of risk must be addressed: you must find a commonly acceptable threshold for all members of the group.

That said, there are different ways of dealing with risk:

- You can **accept** the risk as it stands, because you feel able to live with it
- You can **reduce** the risk, by working on threats, vulnerabilities and capacities
- You can **share** the risk, by undertaking joint actions with other defenders to make potential threats to one defender or organisation less effective
- You can choose to **defer** the risk, by changing your activities or changing approach to reduce potential threats
- You can **escape** risk by reducing or stopping your activities (in some cases, it might imply going into exile)
- You can **ignore** the risk, by turning a blind eye to it. Needless to say, that it is not the best option.

Bear in mind that the level of risk is usually different for each of the organizations and individuals involved in a human rights case, and that attackers usually tend to hit in the weakest parts.

For example:

Let's look at a case of a peasant killed by a landowner's private army. Maybe several organizations and individuals are involved, such as a group of lawyers from the close-by capital city, a local peasant union and three witnesses (peasants who live in a nearby village). It is key to assess the different levels of risk of each of these stakeholders in order to plan properly for the security of each.

Summary

When it comes to security, defenders do not start from zero. They all have devised ways to handle risks and threats. The contrary might imply that they are not around anymore and/or have left their work.

Defenders have at least devised ad hoc deterrence strategies and tactics. Some might also have devised a deterrence global strategy.

Whatever the strategies, they need to respond to at least the following criteria: responsiveness, adaptability, sustainability, effectiveness and reversibility.

A risk assessment must be carried out in order to establish whether it is "acceptable". Otherwise, the defender may reduce, share, differ, escape the risk.

Human rights defenders working in hostile environments

Too often, defenders work in hostile environments. There are many reasons why. Most relate to the fact that defenders' work may lead them to confront powerful actors who are violating international human rights law, be they government or state authorities, security forces, opposition armed groups or private armed gangs. These actors may retaliate by trying to stop defenders doing their work, through anything from subtle repression of attempts at free expression to declared threats and direct attacks. The actors' level of tolerance will depend on the defenders' work - some activities might be deemed acceptable, others not. Often this uncertainty is also deliberate.

Two important considerations should be made here. In many cases, only certain elements **within** complex actors (such as those mentioned above) are hostile towards defenders. For example, some elements within a government may be relatively serious about protecting defenders, while other elements may want to attack them. Defenders may also experience more hostility during times of political upheaval, such as elections or other political events.

Defenders' socio-political work space

This manual focuses on the protection and security of human rights defenders working in hostile environments. Of course action can be taken at the socio-political level: the campaigning and promotion activities of human rights defenders are often aimed at securing a broader acceptance of human rights within society or more effective action from political actors. We don't usually think of such activities as being about security but when successful they can have a positive impact on protecting human rights defenders' **socio-political work space**.

This socio-political work space can be defined as the **variety of possible actions the defender can take at an acceptable personal risk.** In other words, the defender perceives "a broad array of possible political actions and associates a certain cost or set of consequences with each action". The defender perceives some of these consequences as "acceptable and others as unacceptable, thereby defining the limits of a distinct political space"[1].

For instance:

> *A defenders' group may pursue a human rights case until one of the members of the group receives a death threat. If they perceive they have enough socio-political space, they may decide to make public that they have been threatened, and eventually go on with the case. But if they perceive that their political space is limited, they may reckon that denouncing the threat will have unacceptable costs. They might even decide to drop the case for a while and improve their security capacities in the meantime.*

[1] This definition and other key parts of this concept have been taken from Mahony and Eguren (1997), p. 93. They have also developed a model of political space that integrates defenders' work space with the protective accompaniment of defenders.

The notion of "acceptable" risk can change over time and varies greatly between individuals or organisations. For some, torture or the death of a family member might be the most unbearable risk. Some defenders believe that being imprisoned is an acceptable risk, as long as it helps to achieve their goals. For others, the threshold might be reached with the first threat.

This political space of activity, in addition to being subjectively defined by those who move within it, is very sensitive to changes in the surrounding national political environment. You therefore have to look at it as a relative and changeable space.

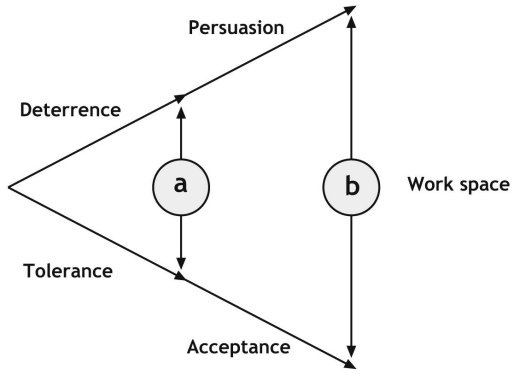
Security and defenders' work space

All security strategies can be summarised in a few words: you want to expand your work space and sustain it in that way. Speaking strictly in security terms, defenders' work space requires at least a minimum level of consent by the main actors in the area - especially by political and military authorities and armed groups who might become affected by defenders' work and decide to act against them.

This consent can be **explicit**, such as a formal permit from the authorities, or **implicit**, for example, in the case of armed groups. Consent will be more solid if the actor can see some benefit resulting from the defenders_ work. It will be lower if the actor perceives related costs. In this case, their level of consent will depend on the political costs carried by an attack on defenders. These issues are especially relevant in armed conflicts where defenders face more than one armed actor. One armed actor might see defenders_ work as helpful to their opponent. Another actor's open acceptance of defenders_ work may therefore lead to hostility by their opponent.

Defenders' work space can be represented by two axes:

- one representing the extent to which the actor will tolerate or accept your work based on the extent to which your work impacts on the actor's objectives or strategic interests (the tolerance-acceptance continuum)
- one representing the extent to which you can deter attacks, because of high political costs, expanding to when you can dissuade the actor on rational/moral grounds or even persuade them of political benefits to not attack you or violating human rights (the deterrence-persuasion continuum).



The expansion of your work space can be achieved over time. Achieving acceptance of defenders' work through a strategy of persuasion should take into account working for the needs of the population, your image, procedures, integration etc, as represented in space "b". But in areas of armed conflict the space usually remains limited to just that which follows from the armed actors' consent, partially generated as a result of the costs of attacking the defenders (deterrence), then having the space reduced to "a".

Generally speaking, space "b" is more likely to be occupied by non contentious defenders than by defenders who openly dennounce abuses. Unless the potential aggressor achieves moral conversion and is persuaded of the goodness of the defender's work to the point of accepting it.

Global security strategy

- Expanding your work space by increasing tolerance and acceptance
- Expanding your work space: increasing deterrence and persuasion

Defining and implementing a global security strategy will contribute to raise the whole political cost of actions against defenders by reduce the level of impunity of potential aggressor and extending the work space of defenders.
Therefore, the global security strategy relies a lot on advocacy.

Expanding your work space by increasing tolerance and acceptance

Your work may affect the objectives or strategic interests of someone who does not care much about human rights, leading to a hostile working environment for defenders. In order to gain acceptance, or at least consent, it is important to limit the confrontation to a strict minimum. Some suggestions for how to do this:

- **Provide information and training about the nature and legitimacy of defenders' work.** Government officials and other actors may be more inclined to cooperate if they know and understand your work and your reasons for undertaking it. It is not enough just for higher officials to be aware of what you do, because defenders' daily work usually involves many levels of officials in different government bodies. You should make a continuous effort to inform and train officials at all levels.

- **Clarify the objectives of defenders' work.** In all conflicts it is useful to clarify and limit the scope and objectives of your work. This will reduce misunderstandings or unnecessary confrontations that can stop defenders achieving their aims.

- **Limit your work objectives to match the socio-political space of your work.** When defenders' work affects an armed actor's specific strategic interests, the actor may react more violently and with less consideration for his image. Some types of work make defenders more vulnerable than others, so make sure your objectives match your risk situation and protection capacities as much as possible.

- **Allow space in your strategies for "saving face".** If you have to confront an actor about human rights abuses seek to leave them a way to gain credit for taking action to address the situation

- **Establish alliances** widely with as many social sectors as possible.

- **Find a balance** between transparency in your work, to show that legitimate defenders have nothing to hide, and the need to avoid giving out information that could compromise your work or security.

- **Finally**, remember that the legitimacy and quality of your work are necessary conditions for keeping your work space open, but that may not be enough. You may also need to be able to deter potential aggressors (see below).

Expanding your work space: increasing deterrence and persuasion

Human rights defenders working in hostile environments should be able to conjure up enough political costs to frighten an aggressor into not attacking them: This is called **deterrence**.

It is useful to distinguish between "general" and "immediate" deterrence. **General deterrence** consists of the combined effect of all national and international efforts at protecting defenders, i.e. anything which helps to create a general understanding that attacks against defenders will have negative consequences. This can happen through wide thematic campaigns or training and information about protecting defenders. On the other hand, **immediate deterrence** sends a specific message to a specific aggressor to keep their attacks away from a specific target. Immediate deterrence is necessary when general deterrence fails or is seen to be insufficient, and when protection efforts are focused on specific cases.

Persuasion is a more inclusive concept. It can be defined as the result of acts which induce an opponent not to carry out a contemplated hostile action. Rational argument, moral appeal, increased cooperation, improved human understanding, distraction, adoption of non-offensive policy and deterrence may all be used to achieve persuasion .Each of these tactics is used at different times by defenders at the national and international levels. Defenders cannot of course use direct "threats" very often: the strategy is more about reminding others that, depending on their decisions, a series of consequences **could** occur.

Putting deterrence to work

In order to measure whether you have been effective in deterrence, a series of conditions must be met:

1 ◆ **Defenders must clearly specify and communicate to the aggressor what types of actions are unacceptable.** Deterrence will not work if the aggressor does not know which actions will provoke a response.

2 ◆ **The defenders' organisation must articulate its commitment to deterring the aggression in a way that makes the aggressor aware of it.** The organisation must also have a deterrence strategy in place.

3 ◆ **The defenders' organisation must be capable of carrying out the deterrence, and make the aggressor aware of this.** If a threat of mobilising national or international reaction is not credible, there is no reason to expect it to have a protective effect.

4 ◆ **Defenders must know who the aggressor is.** Hit squads often work in the dark of night and rarely claim responsibility. This therefore often boils down to analysing who might benefit from an attack. In order to improve the effectiveness of a national or international reaction, an assumption of "state responsibility", although correct, requires more specific information about which factions within the state apparatus are behind the attack.

5 ◆ **The aggressor must have seriously considered attacking and then decided not to carry it out** because the costs - due to the defenders' commitment - would be greater than the benefits.

It is difficult for defenders to dissuade an aggressor who will remain unaffected by a commitment to deter: this happens when governments can be punished by the international community, but cannot in turn punish the actual human rights violator. For example, private armies can be outside the government's reach or don't share its interests. In such cases, the aggressor may even benefit from attacking human rights defenders, because attacks will put the government in a difficult position and harm its image.

Defenders will never know in advance if their "deterrence commitment" is strong enough to dissuade a potential attack. The aggressor may expect benefits that defenders are not aware of. Assessing the situation as carefully as possible is a permanent challenge and may even be impossible due to lack of critical information. Defenders' organisations must therefore develop extremely flexible fallback plans and the ability to respond rapidly to unexpected events.

Table: Preventing a direct aggression – different protection outcomes

PREVENTING A DIRECT AGGRESSION: DIFFERENT PROTECTION OUTCOMES	
1 • **Changes in the perpetrator´s behaviour:** Deterring aggressors by increasing the potential costs of an aggression.	**Confronting** and **reducing threats** (by acting directly against the source, or against any action taken by the source)
2 • **Changes in duty-bearer stakeholders´compliance with the UN Declaration on HRD[2]**: Dissuading aggressors by improving the likelihood of authorities taking action to protect defenders or to punish the perpetrators of an aggression.	
3 • **Reducing the feasibility of the attack:** Reducing defenders' exposure, improving your working environment, managing fear and stress properly, developing security plans, etc.	Reducing **vulnerabilities**, enhancing **capacities**

2 See chapter 1.1. For example, after a defender denounces threats, either the prosecutor or the police or some other body investigates what has happened and this investigation leads to action against those who are threatening the defender. Well, at least this may be the objective of a reaction to prevent an aggression.

CHAPTER 1.7

Preparing a security plan

Purpose:

Learning how to draft a security plan

Drafting a security plan

Now that you have drawn the map of stakeholders in protection, determined the field forces, assessed your risk, recognised your strategies already in place, and established your global strategy, it should not be difficult to draft a security plan.

Security is complex and the combination of several factors. Some must always be present. Others can be added when needed. Together they constitute the security plan.

They need to be implemented at an individual, organisational and inter-organisational level.

How to proceed? Here is a process in just a few steps:

1 ◆ **Components of the plan.** A security plan is aimed at reducing risk. It will therefore have at least three objectives, based on your risk assessment:

- Reducing the level of threat you are experiencing;
- Reducing your vulnerabilities;
- Improving your capacities.

A security plan should include day-to-day policies, measures and protocols for managing specific situations.

Day-to-day policy and measures for routine work

- Permanent advocacy, networking, codes of ethics, culture of security, security management, etc.
- Permanent measures, to ensure that routine work is done in accordance with security standards

Specific situation protocols:

- Preventive protocols: for example on how to prepare a press conference or a visit to a remote area
- Emergency protocols for reacting to specific problems, such as detention or disappearance.

The more day-to-day policies and measures that are implemented, the more the specific situation protocols will work.

Some examples:

- if a permanent set of policies and measures on information management is implemented, an office raid (emergency) will have less impact than where none existed

- if a permanent set of policies and measures on public relations is implemented, an early warning triggered by an attack against a HR defender will be more likely to elicit a reaction from key stakeholders, achieving the objective set by the defender in the event of an attack.

  To achieve the latter, the security plan will include permanent advocacy with duty-bearer and key stakeholders. It will need a permanent ethical behaviour policy operating in all aspects of the organisation's work, as well as the individual/organisational/inter-organisational levels.

- in the event of a detention, if a permanent plan is in place including policy on the ethical behaviour of individuals, then personal breaches of common law may reasonably be excluded as a cause and the emergency protocol can be implemented. Of course, common law infraction could be a pretext, but the organisation's lawyer will know what to do. Furthermore, the detained defender will know that steps are being taken and can recite them to themselves almost to the actual timeline and try and stay calm (psychological impact), knowing that outside action has started. There is no need to challenge the authorities and expose oneself to more risk than what s/he is already undergoing.

- in case of field missions into dangerous areas, relevant key stakeholders will have been previously informed and will be on standby until the team comes back safely.

2 ◆ **Responsibilities and resources for implementing the plan.** To ensure that the plan is implemented, security routines must be integrated into daily work activities:

- Include context assessment and security factors routinely into your schedule
- Register and analyse security incidents
- Allocate responsibilities
- Allocate resources, i.e. time and funds, for security.

3 ◆ **Drafting the plan - how to begin.** If you have done a risk assessment for a defender or organisation, you might have a long list of vulnerabilities, several kinds of threats and a number of capacities. You can't realistically cover everything at the same time. So where should you begin? It's very easy:

- **Select a few threats.** Prioritise the threats you have listed, be they actual or potential, using **one** of these criteria: the most serious threat - clear death threats, for example; **OR** the most probable and serious threat - if organisations similar to yours have been attacked, that is a clear potential threat against you; **OR** the threat which corresponds most to your vulnerabilities - because you are more at risk due to that specific threat.
- **List your relevant vulnerabilities.** These vulnerabilities should be addressed first, but remember that not all vulnerabilities correspond to all threats (see example below)
- **List your relevant capacities.**

Example

of selection process leading to the drawing up of a security plan:

The leader of a defenders' organisation (whether rural or urban) has received serious death threats. The organisation carries out the risk assessment of the threat and lists its vulnerabilities and capacities.

In conclusion, the organisation decides to implement the following security measures: secure all cupboards, fit iron bars to protect the office windows, purchase new cell phones for the members most at risk and publicly decry the death threats.

In general, the point is to ask and demonstrate how each measure is going to contribute to reducing the specific risk (in other words, how it is going to increase the security related to the specific risk)?

So: how are all these measures going to actually reduce the specific death threat against the leader? (Of course, they might address the global security of the organisation but this is not the right time to deal with it).

Ask yourself: What is the likelihood of the death threat being carried out at the office knowing that there are people around? Does the leader need to be at the office to be killed? The threatened leader will not always be at the office. So, there are other many other vulnerabilities, such as leaving the office alone late at night, or travelling to isolated areas, ignoring security measures whilst at home...

Although securing cupboards is important, it will not reduce the threat and vulnerabilities to the leader. The same goes for the iron bars on the windows. What could they do against a sniper and or a grenade?

How is a cell phone going to reduce that risk? (what can actually be done with a cell phone to prevent someone from killing the leader?)

It may be more useful to reduce the leader's exposure while commuting from home to the office or at weekends. These are the vulnerabilities that need to be addressed first as they are far more relevant to such a threat.

If the process selection is correct and you are in a position to address the selected threats, vulnerabilities and capacities in your security plan, you can be reasonably be sure that you will be able to reduce your risk from the right starting point.

Please note that this is an *ad hoc* way of drafting a security plan. There are more "formal" ways to do it, but this method is straightforward and makes sure you take care of the most urgent security issues - provided your risk assessment is correct - and end up with a "live" and "real" plan at the end: that is the important part of security. *(Please see the end of this Chapter for a detailed list of possible security plan components which you can also use when assessing your risks.)*

Possible factors to include in a security plan

This "menu" details suggestions for factors to include in a security plan. After carrying out a risk assessment, you can pick and mix these ideas to complete your security plan.

A security plan includes elements that become political procedures (like meeting the authorities and international bodies, claiming the protection due from the state) and operational procedures (such as routine preparations for a field mission).

Elements of permanent policies and measures for the ordinary work:

- The organisation's mandate, mission and general objectives.
- An organisational statement on security policy.
- Security should cut across all aspects of daily work: context assessment, risk assessment and incident analysis, as well as security evaluation.
- How to ensure that all organisation members are properly trained in security to the required level and that people's security responsibilities are passed on when they leave the organisation.
- Allocation of responsibilities: Who is expected to do what in which situation?
- How to handle a security crisis: Setting up a crisis committee or working group, delegating responsibility for handling the media, communicating with relatives, etc.
- Organisational security responsibilities: Planning, follow-up, insurance, civil responsibility, etc.

- Individual security responsibilities: continuing to reduce risk, how to handle free time or leisure activities, reporting and recording security incidents, sanctions (some of these points could be included in work contracts, where relevant).

- Organisational policies on:
  - rest, free time and stress management
  - the security of witnesses
  - health and accident prevention
  - links with authorities, security forces and armed groups
  - information management and storage, handling confidential documents and information
  - your own image in relation to religious, social and cultural values
  - security management in offices and homes (including for visitors)
  - handling cash or valuables
  - communication means and protocols
  - vehicle maintenance

Elements of specific measures for extraordinary work and situations

- Prevention and reaction protocols:
  - preparing field trips
  - landmines
  - reducing the risk of getting involved in common crime, armed incidents or sexual attacks
  - reducing the risk of accidents when travelling or in risky areas
  - reaction protocols on: medical and psychological emergencies (also in the field)
  - personal injury, attacks , including sexual attacks
  - robbery
  - when a person does not show up when they are supposed to
  - arrest or detention
  - abduction, disappearance
  - fire and other accidents
  - evacuation
  - natural disasters
  - legal or illegal searches or break-ins into offices or homes
  - if a person comes under fire
  - if someone is killed
  - in the event of a Coup d'État

Implementing a security plan

Security plans are important, but they are not easy to implement. Implementation is much more than a technical process - it is an organisational process. This means looking for entry points and opportunities, as well as barriers and problems.

A security plan must be implemented on at least three levels:

1 ◆ The **individual** level. Each individual has to follow the plan in order for it to work.

2 ◆ The **organisational** level. The organisation as a whole has to follow the plan.

3 ◆ The **inter-organisational** level. Some level of cooperation between organisations is usually involved to maintain security.

Examples

of **entry points** and **opportunities** when implementing a security plan:

- Several minor security incidents have taken place in your own or another organisation and some staff members are worried about it.
- General security concerns exist because of the situation in the country.
- New staff arrives and can be trained to start good security practices more easily.
- Another organisation offers you security training.

Examples

of **problems** and **barriers** to implementing a security plan:

- Some people think more security measures will lead to an even greater workload.
- Others think the organisation already has good enough security.
- "We haven't got time for this stuff!"
- "OK, let's make extra time to discuss security on Saturday morning, but that's it!"
- "We need to take better care of the people we intend to help, not ourselves."

Ways of improving the implementation of a security plan

- **Take advantage of opportunities and entry points** to face problems and break through barriers.

- **Proceed step-by-step.** There's no point in pretending that everything can be done at once.

- **Emphasise the importance of security to core work on behalf of victims.** Stress that the security of witnesses and family members is critical to the effectiveness of core work and that this can best be managed by integrating good security practices into all areas of work. Use examples in training/discussion that demonstrate the potential negative impact of lax security on witnesses and victims.

- A plan drafted by two "experts" and presented to a whole organisation is likely to fall flat on its face. In security, **participation is key.**

- **A plan must be realistic and feasible.** A long list of things to do before every field trip will not work. Keep to the bare minimum necessary to ensure security. This is another reason to involve those who really do the work - for example, people who usually go on field trips.

- **The plan is not a one-off document** - it must be reviewed and updated all the time.

- **The plan must not be seen as "more work", but as "a better way to work".** People must be made to see the benefits, for example, by avoiding duplicate reporting. Make sure field trip reports have a security dimension, make security issues part of normal team meetings, integrate security aspects into other training, etc.

- **Emphasise that security is not a personal choice.** Individual decisions, attitudes and behaviour that impacts on security can have consequences for the security of witnesses, family members of victims and colleagues. There needs to be a collective commitment to implementing good security practices.

- **Time and resources must be allocated** to implementing the plan, as security cannot be improved by using people's free time. In order to be seen as "important", security activities must be placed alongside other "important" activities.

- **Everyone must be seen to follow the plan,** especially managers and those responsible for other people's work. There must be consequences for individuals who persistently refuse to abide by the plan.

Summary

A security plan has to decrease vulnerabilities and increase capacities so that threats are being reduced or made less feasible and therefore the risk is reduced.

A security plan must fit your actual needs and work space.

The point is not necessarily to cover a big socio-political space -rather to be within the right space and to cover as much of the working environment as possible, through networking and in conjunction with other organisations. Establish security procedures that transcend political differences.

Security is the concern of all and it is individual, organisational and inter-organisational.

Security is complex and is the result of several factors. Some must always be present. Others will be added at specific moments. Together they constitute the security plan.

Your security plan should include day-to-day policies, measures and specific situation protocols.

Both include political procedures and operational procedures.

CHAPTER 1.8

Improving security at work and at home

Purpose:

Assessing security at work or at home.

Planning, improving and checking security in offices and homes.

Security at work and at home

Security at the organisation's headquarters or offices and in staff members' homes is of fundamental importance to human rights defenders' work. We will therefore go into some depth about how the security of an office or home can be analysed and improved. *(For the sake of simplicity we will only refer to "offices" from now on, although the information below also applies to home security.)*

General aspects of office security

Our aim in improving security can be summarised in three words: **Prevent unauthorised access.** This is true whether your office is in an urban or rural area. In rare cases it may also be necessary to protect an office against a possible attack (against bombing, for example).

This brings us to the first general consideration - the vulnerabilities of an office. They increase risk, depending on the threat you face. For example, if you are at risk of someone stealing equipment or information, you must remove your vulnerabilities accordingly. A night alarm (electric, if you have access to electricity, or a night watchman, or otherwise a dog) is of little use if nobody is going to come and check what has happened. On the other hand, if there is a violent break-in in daylight, reinforced door railings or alarms won't be very useful. In short, take measures according to the threats you face and the context you are working in.

The vulnerabilities of an office must be assessed in the light of the threats you may face.

However, it is important to find a balance between putting appropriate security measures in place and giving outsiders the impression that something is being "hidden" or "guarded", because this can in itself put you at risk. In office security you often have to choose between keeping a low profile or taking more obvious measures if need be. On the other hand, a potential aggressor will be aware that your office contains valuables or contentious information and that you 'need' to protect it.

The security of an office is no greater than its weakest point.

If somebody wants to gain entry without your knowledge, they won't choose the most difficult entry point. Remember that the easiest way of gaining access to an office and observing what goes on inside is, sometimes, as simple as knocking on the door and getting inside.

The office location

Whether the office is in an urban or rural area, the factors to consider when setting up an office are: the neighbourhood; whether the building is associated with any particular people or activities from the past; accessibility of public and private transport; risk of accidents; how suitable the building is for putting the necessary security measures in place, etc. *(Also see Location evaluation risk below.)*

It is useful to review which security measures are being taken by others in the neighbourhood. If there are many, this may be a sign of an unsafe area, for example, in respect of common crime. It is also important to talk to people in the area about the local security situation. In any case, make sure security measures can be taken without attracting undue attention. It is also useful to get to know local people as they can pass on information regarding anything suspicious going on in the neighbourhood.

It is also important to check out who the owner is. What reputation do they have? Could they be susceptible to pressure from the authorities? Will they be comfortable with you putting security measures in place?

The choice of office must take account of who needs to come to the office. An office where victims come to seek legal advice will have different requirements to an office which is primarily a place for staff to work. It is important to take account of how easy it is to get to by public transport, will it result in unsafe journeys between the area where staff live, those where most work activities take place, etc. The surrounding areas must be evaluated, especially in order to avoid having to travel through unsafe areas.

In some cases, the office may simply be the defender's house (see rural area below). Yet, the above consideration must be given.

Once the location has been selected, it is important to undertake periodic evaluations of aspects of the location which can vary, for example if an 'undesirable element' moves into the neighbourhood.

Checklist for choosing a good office location in served areas	
Neighbourhood:	Crime statistics; closeness to potential targets of armed attacks, such as military or government installations; secure locations for taking refuge; other national or international organisations with whom you have a relationship.
Relationships:	Type of people in the neighbourhood; owner, former tenants; former uses of the building.
Accessibility:	One or several good access routes (the more, the better. But remember that the undesired element will also have a greater choice); accessibility by public and private transport.
Basic services:	Water and electricity, phone.
Street lighting	In the surrounding area.
Susceptibility to accidents or natural risks:	Fires, serious flooding, landslides, dumping of dangerous materials, factories with hazardous industrial processes, etc.
Physical structure:	Solidity of structures, facility for installing security equipment, doors and windows, perimeter and protection barriers, access points (see below).
For vehicles:	A garage or at least a courtyard or enclosed space, with a parking barrier.

In case the office is located in a secluded, remote and badly served area, the result of the check list might indicate that several of the items do not exist in the area. Capacities will need to be developed to compensate for specific vulnerabilities. For example, if there are no other organisations around, you might consider resorting to the local community. Or, in case of no running water or extinguisher: make sure you have a big enough water recipient always full.

Third-party access to the office: physical barriers and visitor procedures

You now know that the primary purpose of office security is denying unauthorised people access. One or several people could enter to steal, acquire information, plant something which can later be used against you, such as drugs or weapons, threaten you, etc. Every case is different, but the aim remains the same: Avoid it.

Access to a building is controlled through **physical barriers** (fences, doors, gates), through **technical measures** (such as alarms with lighting) and **visitor admission procedures.** Every barrier and procedure is a **filter** through which anyone who wishes to gain access to the office must pass. Ideally, these filters should be combined to form several layers of protection, capable of preventing different types of unauthorised entry.

Physical barriers.

Barriers serve to **physically** block the entry of unauthorised visitors. How useful physical barriers are depends on their **solidity** and ability to cover **all vulnerable gaps** in the walls.

Your office can have physical barriers in three areas:

1 ◆ The **external** perimeter: Fences, walls or similar, beyond a garden or courtyard. In the absence of external physical perimeter, you may define the extension of external perimeter that you will keep under control.

2 ◆ The perimeter of the **building or premises.**

3 ◆ The internal perimeter: Barriers which can be created within an office to protect one or several rooms. This is particularly useful in offices with many visitors passing through, as it allows for a separate public area and a more private one which can be protected with additional barriers.

The external perimeter

The office should be surrounded by a clear external perimeter, possibly with high or low fences, preferably solid and high to make access more difficult. Railings or see-through wire mesh will make the organisation's work more visible, and it is therefore better to have brick walls or similar.

In the absence of clear external fenced perimeter, you can decide how much external extension you can visually control so as to be able to see undesirable elements getting closer to your office. You might consider using convex mirrors.

The perimeter of the building or premises

This includes walls, doors, windows and ceiling or roof. If the walls are solid, all the openings and the roof will also be solid. Doors and windows must have adequate locks and be reinforced with grills, preferably with both horizontal and vertical bars well embedded into the wall. If there is a roof, it should offer good protection - not just a simple sheet of zinc or a layer of tiles. If the roof cannot be reinforced, block all possible access to the roof from the ground or neighbouring buildings.

If your office window faces the street or a public space, place your desk in such a way that you can see but not be seen. If it faces vegetation, make sure that no one can hide behind it unseen.

Some offices might have more doors and therefore one may serve as "emergency exit". Remember that an emergency exit may also become an entry point for undesired elements

In a location with a risk of armed attack, it is important to establish secure areas within the office (see in this Manual the chapter on security in areas of armed conflict).

The internal perimeter

The same applies here as to the building or premises. It is very useful to have an area with additional security inside the office, and this is usually very easy to arrange. Even a safety deposit box can be considered an internal security perimeter.

Your office might be made of one room only in which case, you might consider the possibility to use mobile screens/partitions to keep private space away from the visitor sight.

A note on keys

- No keys should be visible or accessible to visitors. Keep all keys in a cupboard or drawer with a simple combination lock for which only a few group members know the code.. Make sure that the code is changed from time to time for greater security.
- If keys are individually labelled, do not mark them with a description of the corresponding room, cupboard or drawer, as this will make a robbery much easier. Use number, letter or colour coding instead.

Technical measures: Lighting and alarms

(in case your office has got access to electricity service or is equipped with an electricity generator).

Technical measures strengthen physical barriers or visitor admission procedures (such as spy holes, intercoms and video cameras. See below). This is because **technical measures are only useful when they are activated to deter intruders.** In order to work, a technical measure must provoke a particular reaction, for example, attracting attention from neighbours, the police or a private security firm. If this does not happen, and the intruder knows that it won't, such measures are of little use and will be reduced to preventing petty theft or recording the people who enter.

- **Lighting** around the building (of courtyards, gardens, pavement) and on landings is essential.
- **Alarms** have several purposes, including detecting intruders and deterring potential intruders from entering or from continuing to attempt access.

An alarm can activate a warning sound inside the office; a security light; a general, loud tone, bell or noise; or a signal in an external security centre. An audio

alarm is useful for attracting attention but can be counter-productive in conflict situations or if you don't expect local residents or others to react to it. A careful choice must be made between an audio and light alarm (a fixed powerful light, and an intermittent red light). The latter can be enough to deter an intruder, because it suggests that something else will happen following initial detection.

Alarms should be installed at access points (courtyards, doors and windows, and vulnerable premises such as rooms containing sensitive information). The most straightforward alarms are **motion** sensors, which activate a light, emit a noise or activate a camera when they detect movement.

- Alarms should:
  - have a battery, so they can function during power cuts;
  - have a delay before the activate so they can be deactivated by staff who might set them off accidentally;
  - include an option for manual activation in case staff need to turn them on;
  - be easy to install and maintain;
  - be easily distinguishable from a fire alarm.

Video cameras

Video cameras can help improve admission procedures (see below) or record people who enter the office. However, the recording must be made from a point which is beyond the reach of an intruder. Otherwise intruders can break open the camera and destroy the tape.

You may need to consider whether cameras will intimidate people you want to come and visit you such as victims or witnesses, or whether they will be seen as a valuable commodity which will attract thieves. It is good practice to post a warning notice if you are using a camera (the right to privacy is also a human right).

Lighting and alarms in case your office does not have access to electricity service or is not equipped with an electricity generator.

Simply avoid staying at your office once it is dark.

The electric alarm can be substituted with other alarm system: a night watch man, neighbours, family, community, dogs: Get their support and see how they can become your alarm system.

Private security companies

This area requires great care. In many countries, private security firms are staffed by ex-security force members. There are documented cases of such people being involved in surveillance of, and attacks on, human rights defenders. It therefore makes sense not to trust security companies if you have reason to fear

surveillance or attacks by security forces. If a security company has access to your offices, they could plant microphones or allow other people in.

If you feel you need to use a security company you should ensure that you have a clear agreement about what their personnel are allowed to do, and not allowed to do on your behalf, and which parts of the building they can access. Of course, you also must be able to monitor that these agreements are fulfilled.

For example:

> *If you have hired a security service that sends a guard in case an alarm breaks off, this guard may have access to sensitive parts of your office and might set up listening devices in your meeting room.*

It is better if you can agree (and if possible screen) which specific staff will be working for you, but this is rarely possible.

If the security guards carry weapons it is important for the human rights organization to have a clear understanding about what their rules are for using them. But it is even more important to weigh the potential benefits of using weapons against their drawbacks. Hand guns are not a deterrence against attackers with higher fire capacity (as it is usually the case), but if attackers know that there are carriers of shot guns within your premises, they may decide to break in ready to open fire, to protect themselves during the attack. In other words, some armed capacity (small arms) will probably lead attackers to open use of arms with higher fire capacity. At this point it is worth asking yourself: if you need guards with sub-machine guns, do you have the minimum socio-political space in which to carry out your work?

Admission procedure filters

Physical barriers must be accompanied by an **admission procedure** "filter". Such procedures determine when, how and who gains access to any part of the office. Access to sensitive areas, such as keys, information and money, must be restricted.

The easiest way to gain entry to an office where human rights defenders work is to knock on the door and get inside. Many people do this every day. In order to reconcile the open character of a human rights office with the need to control who wants to visit you and why, you need appropriate admission procedures.

In general, people have a particular reason to want to enter or knock on your door. They often want to ask a question or to deliver something, without necessarily asking permission first. Let's examine this case by case:

Someone calls and asks for permission to enter for a particular reason.

You should then follow three simple steps:

1 ◆ **Ask why the person wishes to enter**. If s/he wants to see somebody in the office, consult the latter. If that person is not present, ask the visitor to return at another time or to wait somewhere outside the restricted office area. It is important to use spy holes, cameras or entry phones

to avoid having to open or approach a door, especially if you want to refuse someone entry or are facing violent or forced entry. It is therefore good to have a waiting area which is physically separate from the office's internal entrance. If an easily accessible public area is essential, ensure that there are physical barriers blocking access to restricted parts of the office.

Someone could request entry in order to check or repair the water or electricity supply or carry out other maintenance work. S/he could also claim to be a media representative, a state official, etc. Always confirm their identity with the company or organisation they claim to be representing before allowing them entry. Remember that neither a uniform nor an identity card are guarantees of proper and secure identification, especially in a medium or high-risk situation.

2 ◆ **Decide whether or not to allow access.** Once your visitor's reason for entering has been established, you'll need to decide whether or not to allow them in. Just because someone states a reason for entering isn't a good enough reason to let them in. If you are not sure what their errand is, don't allow access.

3 ◆ **Supervise visitors until they leave.** Once a visitor has entered the office, make sure that someone is supervising them at all times until they leave. It is useful to have a separate area to meet with visitors, away from the restricted areas.

A record should be kept of every visitor with name, organization, purpose of visit, who they met with, time at which they arrived and left. This can be particularly useful when reviewing what went wrong after a security incident.

Someone arrives or calls asking questions.

Regardless of what a caller or visitor might say, you should under no circumstances tell them the location of a colleague or other people nearby, nor give them any personal information. If s/he is insistent, offer to leave a message, ask them to come or call back later or make an appointment with the person they wish to see.

People can often show up mistakenly, asking if so-and-so lives there or if something is for sale, etc. Some also want to sell things, and beggars can come looking for help. If you deny these people access and information, you will avoid any security risk.

Someone wants to deliver an object or package.

The risk you run with a package or object is that the contents could compromise or hurt you, especially in case of a package or letter bomb. No matter how the innocent it may look, do not touch or handle a package until you have taken these three simple steps:

1 ◆ **Check if the intended recipient is expecting the package.** It is not enough that the recipient knows the sender, because the sender's iden-

tity could easily be faked. If the intended recipient is not expecting a package, s/he must check that the supposed sender has actually sent them something. If the package is simply addressed to your office, check who sent it. Wait and discuss the issue before making a final decision.

2 ◆ **Decide whether or not to accept the package or letter.**
If you can't establish who sent the package, or if this will take time, the best option is not to accept it, especially in a medium or high risk environment. You can always ask for it to be delivered later, or collect it at the post office.

3 ◆ **Keep track of the package inside the office.** Make sure you know where in the office the package is, at all times until the recipient accepts it.

In some countries, a package is announced over the phone and it is the defender who has to go and pick it up. It might be a trick to attract the defender and expose them to aggression. As the phone might not be registered, it is impossible to track the caller down. Once the defender has enquired about the origin of the package, they can check the information with the alleged sender and ask them the route of the package. Then, the defender can decide whether it is safe to go and pick it up or not. They can also ask the caller to bring round to the office and follow the above procedures. Most probably, if it is a pretext, the caller will abstain from turning up at the office.

During functions or parties.

In these circumstances, the rule is simple: Do not let anyone whom you don't know first hand enter. Only people who are known to trusted colleagues should enter, and only when that colleague is present and can identify their guest. If a person shows up saying they know someone in the office check the information the person being mentioned and if s/he isn't there, don't let them in.

Defenders might hesitate and find it difficult to enquire about a visitor and send them away. However, they don't need to proceed on their own account. They can simply say that they are not authorised to let the visitor in.

Also, for all visitor admission procedures, remember that if the visitor is genuine, they will appreciate the care the organization takes in security and if the visitor is not genuine, they are aware that they also implement security procedures. So, whatever the case, defenders can simply give themselves the authority to deny entry to the unknown visitor. If it helps, they can use a "no and...": I am not authorized to let unknown visitors in however, if you care to leave your visit card, I will be pleased to inform you of future public events we might organise".

Keeping records of phone calls and visitors.

It may also be useful to keep a record of phone calls, phone numbers and visitors (in some organizations, new visitors are requested to present an identity document and the organization registers the number of the document).

Working extra hours at the office.

There should be procedures for staff working extra hours. Members of an organization intending to work extra hours late at night should report by certain hours with another designated member, take special care when leaving the premises, etc.

Checklist: Identifying weak points in admission procedures
◆ **Who** has regular access to **which** areas and **why**? Restrict access unless it is absolutely necessary.
◆ Distinguish between different **types** of visitors (messengers, maintenance workers, computer technicians, NGO members for meetings, VIPs, guests for functions, etc,) and **develop appropriate admission procedures for each**. All staff should be familiar with all procedures for all types of visitors, and take responsibility for carrying them out.
◆ Once a visitor enters the office, can they access weak points? Develop strategies to prevent this.
Checklist: Access to keys
◆ **Who** has access to **which** keys and **when**?
◆ Where and how are **keys** and **copies** of those **kept**?
◆ Is there a **record of key copies** that are in circulation?
◆ Is there a risk that somebody will make an **unauthorised key copy**?
◆ What happens **if somebody loses a key**? The corresponding lock must be changed, unless you are absolutely sure that it has been accidentally mislaid and that nobody can identify the owner of the key or your address. Remember that a key can be stolen – for example, in a staged robbery – in order for someone to gain access to the office.

All staff members have a responsibility to take action against anyone who is not properly observing the admission procedures. They should also make a note in the security incidents book of any movements by suspicious people or vehicles. The same applies to any object placed outside the building, in order to rule out the potential risk of a bomb. If you suspect a bomb, don't ignore it, **don't touch it,** and do contact the police.

When moving offices, or if keys have been lost or stolen, it is essential to change all the locks in the entrance area, at the very least.

Checklist: General office security procedures

- ☐ Provide fire extinguishers and flashlights (with replaceable batteries). Make sure all staff members know how to use them.
- ☐ Provide an electricity generator if there is a strong possibility of power cuts. Power cuts can endanger security (lights, alarms, telephones, etc.), particularly in rural areas.

- Keep a list handy of local emergency numbers for police, fire brigade, ambulance, nearby hospitals for emergencies, etc.
- If there is a risk of conflict nearby, keep a supply of food and water in reserve.
- Establish the location of secure areas outside the office for emergencies (for example, the offices of other organisations).
- Nobody from outside the organisation must be left **alone** in a vulnerable area with access to keys, information or valuables.
- **Keys:** Never leave keys where visitors might have access to them. Never "hide" keys outside the office entrance – this makes them accessible, not hidden.
- **Admission procedures:** Security barriers offer no protection if a potential intruder is allowed to enter the office. The main points to bear in mind are:
  - All group members are equally responsible for visitor control and admission.
  - All visitors must be accompanied at all times while in the office.
- If an unauthorised visitor is found in the office:
  - Never confront someone who seems prepared to use violence to get what they want (for example, if they are armed). In such cases, alert colleagues, find a safe place to hide and try to get help from the police.
  - Approach the person carefully or seek assistance in the office or from the police.
- In high risk situations, always keep control of vulnerable things, such as the information stored on a hard drive, in order to make them inaccessible or remove them in case of an emergency evacuation.
- Bear in mind that in case of confrontation with a potential intruder, the people working in the office are on the front line. Ensure that they have the necessary training and support at all times to deal with any situation, and without putting themselves at risk.

Regular inspections of office security

Regular supervision or inspection of office security is very important, because security situations and procedures vary over time, for example, because equipment deteriorates or if there is a high staff turnover. It is also important to achieve some sense of staff ownership of the office security rules.

The person responsible for security must carry out at least one review of office security **every six months.** With the help of the list below this can take as little as one or two hours. The person in charge of security must ensure that staff feedback is sought before the final report is written, and then present the security report to the organisation in order for the necessary decisions to be made and for action to be taken. The report should be kept on file until the next security review.

Checklist: Office Security Review

Review of:
Carried out by:
Date:

1 ◆ **Emergency contacts:**

- Is there a handy and up to date list with telephone numbers and addresses of other local NGOs, emergency hospitals, police, fire brigade and ambulance?

2 ◆ **Technical and physical barriers (external, internal and interior):**

- Check condition and working order of external gates/fences, doors to the building, windows, walls and roof.
- Check condition and working order of external lighting, alarms, cameras or video entrance phones.
- Check key procedures, including that keys are **kept securely** and **code-labelled,** assignment of **responsibility** for controlling keys and copies, and that keys and copies are in **good working order**. Make sure **locks** are changed when keys are lost or stolen, and that such incidents are **logged.**

3 ◆ **Visitor admission procedures and "filters":**

- Are admission procedures in operation for all types of visitors? Are all group members and staff familiar with them?
- Review all recorded security incidents related to admission procedures or "filters".
- Ask those staff members who usually carry out admission procedures if the procedures are working properly, and what improvements are needed.

4 ◆ **Security in case of accidents:**

- Check the condition of fire extinguishers, gas valves/pipes and water taps, electricity plugs and cables and electricity generators (where applicable).

5 ◆ **Responsibility and training:**

- Has responsibility for office security been assigned? Is it effective?
- Is there an office security training programme? Does it cover all the areas included in this review? Have all new staff members been trained? Is the training effective?

In rural areas:

Defenders also work in rural areas either in a village or in a secluded and remote area. They might not have much choice as to their office location. Yet they need to protect their space from unwanted visitors and objects.

Village: if it is comparable to a micro urban area most of the above considerations may be taken and completed with the following ones.

Remote and secluded location: make sure that the surrounding community, your family and friends can contribute to your alarm system. Try and have them check regularly on you and your office (whether it is your home). You might consider keeping a dog which can be trained to barking at visitors. Make sure it doesn't attack people and that it cannot easily be approached and poisoned.
Get to the area well and avoid being out at dark.
You might consider establishing communication relays through trusted people to have access to as quick a supportive reaction as possible in case you need it.

Summary

The aim of office/home security measures is to reduce the risk of unwanted access

The security of an office is no greater than its weakest point.

Whether your office/home is located in an urban or rural area, you can use the equation in order to reducing the risk of unwanted access.

Threats might be assimilated to consequences.

List all your threats/consequences of the risk of unwanted access. Then, per threat/consequence, list respective vulnerabilities and capacities and work on them.

CHAPTER 1.9

Security for women human rights defenders

Purpose:

Looking at security from the perspective of women human rights defenders

Providing both women and men human rights defenders with additional security/protection knowledge and tools

Introduction

Although the security of women human rights defenders' is interrelated with the security of all human rights defenders, we have decided to dedicate a specific chapter to the security of women human rights defenders, because experience in the field shows that it is not systematically mainstreamed. There are multiple reasons for this and, ultimately they mostly originate from the social, cultural and religious context[1]. This is why we have elected to introduce the topic with a short compilation of comments gathered directly from experience in the field which highlights the convergence of interests and the necessary collaboration between women and men human rights defenders.

Women human rights defenders

Women have always been important stakeholders in the promotion and protection of human rights. However, their role is not always acknowledged. Women work on their own or alongside with men in the defence of human rights.

Unfortunately, too often:

- they face not only gender-related violence outside their organisations but also gender prejudice and discrimination within human rights defenders' organisations themselves.

- there is often an excuse to "postpone" women's rights on the agenda or make it an "extraordinary" agenda item, as if there was a priority order instead of interdependence with human rights. This happens in mixed human rights defenders organisations.

1 Ethic of Care

- women human rights defenders are still considered by their male peers as auxiliaries. Male peers will often refuse tasks regarded as less fundamental, as if their masculinity depended on it.

Sexism, classism, racism, 'casteism', xenophobia and homophobia are all more or less subtle facets of the same logic underlying human rights violations against men, women, people of different sexual orientation, children, elderly, ethnic groups, poor people... They all have an impact on security: for example, in some places, pariahs are not considered at all within the security plan: neither positively (i.e. as people aware of their surroundings) nor negatively (i.e. as potential aggressor's informers).

The concept of violence is often twisted:

- fighting "violence against women" instead of fighting male violence
- "domestic violence" as a euphemism for male violence.

By working on putting an end to male violence, domestic violence should drop as a result. They are not separate issues.

Women are often still considered lesser human beings, although modern science has established that gender differences do not imply an order value. It sounds obvious but experience in the field and in workshops with defenders has shown that this idea is not necessarily integrated. This explains our insistence.

Since women have had access to school and education they have proved to be just as intelligent as men (only to mention the use of intelligence at school). There is often confusion between intelligence and access to information. The same can be said for ethnic minorities and any other discriminated against group: it is not a anthropological question, rather a social one. An educated individual/group might engage in a peer and substantiated dialectic and challenge the establishment. This might explain why too many girls and women are still not allowed to access education.

Women notice the contradiction between defending human rights on the one hand and discriminating against women on the other. Inevitably, sometimes, women would like to tell their male peers to go back to square one and come back once they are aware of it and are ready to change their behaviour. However, women stay and keep working alongside their male colleagues: more women join human rights' actions organised by men, than men do women's rights actions organised by women.

Where violence is perpetrated against women, be it against even one woman (or any other group or individual), it is not an issue of culture or religion but of power.

In the case of Nelson Mandela and Desmond Tutu for example, apartheid did not end because the dignity of black people was suddenly recognised, but because

some white people recognised they had lost theirs. The same can be applied to gender-based discrimination and to any other type of discrimination.

As long as male human rights defenders fail to see that gender-based discrimination originates from the same perverse logic that legitimises all the other types of discrimination, then the human rights defenders movement will be half the strength it could potentially be. Also, it will continue to serve the purposes of the human rights violators: to divide and rule.

Women's rights are not just women's rights .

This chapter does not attempt to change minds and values, but to see how gender-based and all other types of discrimination impact on the security and protection of women firstly, but also of male human rights defenders. Thus, whilst a change in mindset may be too ambitious an aim, deterrence is not and this involves changes in behaviour. In this case, male solidarity on issues of women's security contributes to the security of all human rights defenders.

More material has been produced in the context of the International Consultation on Women Human Rights defenders-Colombo- Sri Lanka, 2005[1].

http://defendingwomen-defendingrights.org/pdf/WHRD-Proceedings.pdf

Attacks on women human rights defenders

In her **2002 annual report to the Commission on Human Rights** Hina Jilani, the UN Secretary General's Special Representative on Human Rights Defenders stated:

> *Women human rights defenders are on a par with their male colleagues in putting themselves on the front line in the promotion and protection of human rights. In doing so, however, as women, they face risks that are specific to their gender and additional to those faced by men.*
>
> *In the first instance, as women,* ***they become more visible.*** *That is, women defenders may arouse more hostility than their male colleagues because as women human rights defenders they may defy cultural, religious or social norms about femininity and the role of women in a particular country or society. In this context, not only may they face human rights violations for their work as human rights defenders, but even more so because of their gender and the fact that* ***their work may run counter to societal stereotypes*** *about women's submissive nature, or challenge notions of the society about the status of women.*

[1] A very useful guide on women human rights defenders UNHCHR website at http://www.unhchr.ch/defenders/tiwomen.htm Also see *Report: Consultation on Women HRDs with the UN Special Representative of the Secretary General on Human Rights Defenders, April 4-6 2003,* Published by Asia Pacific Forum on Women, Law and Development, and *Essential actors of our time. Human rights defenders in the Americas,* by Amnesty International.

Secondly, it is not unlikely that the hostility, harassment and repression women defenders face may themselves take a gender-specific form, ranging from, for example, verbal abuse directed exclusively at women because of their gender to sexual harassment and rape.

In this connection, ***women's professional integrity and standing in society can be threatened and discredited*** *in ways that are specific to them, such as the all too familiar pretextual calling into question of their probity when - for example - women assert their right to sexual and reproductive health, or to equality with men, including to a life free from discrimination and violence. In this context, for example, women human rights defenders have been tried using laws criminalizing conduct amounting to the legitimate enjoyment and exercise of rights protected under international law on spurious charges brought against them simply because of their views and advocacy work in defence of women's rights.*

Thirdly, human rights abuses perpetrated against women human rights defenders can, in turn, have repercussions that are, in and of themselves, gender-specific. For example, ***the sexual abuse*** *of a woman human rights defender in custody and her* ***rape can result in pregnancy and sexually transmitted diseases, including HIV/AIDS.***

Certain women-specific rights are almost exclusively promoted and protected by women human rights defenders. Promoting and protecting women's rights can be an additional risk factor, as the assertion of some such rights is seen as a threat to ***patriarchy and as disruptive of cultural, religious and societal mores.*** *Defending women's right to life and liberty in some countries has resulted in the life and liberty of women defenders themselves being violated. Similarly, protesting against discriminatory practices has led to the prosecution of a prominent women's rights defender on charges of apostasy.*

Factors such as age, ethnicity, educational background, sexual orientation and marital status must also be taken into consideration, as different groups of women defenders face different challenges and therefore have different protection and security needs.

The assessment of the protection needs of women defenders will help to clarify their specific and often different vulnerabilities and coping strategies. They can thus be more adequately addressed in emergency and day-to-day situations.

THE DECLARATION ON THE ELIMINATION OF VIOLENCE AGAINST WOMEN (1993) DEFINES VIOLENCE AGAINST WOMEN AS:

Any act of gender-based violence that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts, coercion orarbitrary deprivation of liberty, whether occurring in public or in private life. (Article 1)

Violence against women shall be understood to encompass, but not be limited to, thefollowing:

a) • Physical, sexual and psychological violence occurring in the family, including battering, sexual abuse of female children in the household, dowry-related violence, marital rape, female genital mutilation and other traditional practices harmful to women, non-spousal violence and violence related to exploitation.

b) • Physical, sexual and psychological violence occurring within the general community, including rape, sexual abuse, sexual harassment and intimidation at work, in educational institutions and elsewhere, trafficking in women and forced prostitution.

c) • Physical, sexual and psychological violence perpetrated or condoned by the State, wherever it occurs. (Article 2)

Security of women human rights defenders

Women human rights defenders are paying a heavy price for their work in protecting and promoting other people's human rights. Women defenders have to confront gender-specific risks, and their security therefore requires a specific approach.

The causes will need to be taken into account in the security organisational policies and protocols. Here is a non exhaustive list of causes mentioned in the 2002 Hina Jilani report mentioned above.

- *Women may attract unwanted attention.*
- *Women defenders may have to break patriarchal laws and social taboos.*
- *There are specific forms of aggression against women defenders.*
- *Women defenders may come under pressure to "prove" their integrity.*
- *Male colleagues may not understand, or could even reject, women defenders' work.*
- *Women defenders may experience domestic violence.*
- *Women defenders usually have additional family obligations*
- *All these pressures place an additional burden of work and stress on women defenders.*

Towards better security and protection for women human rights defenders

Global permanent security policies and measures

Mainstreaming women's participation

In a nutshell, this means ensuring full participation by women alongside men in decision-making processes; putting women's security issues on the agenda, and placing women on a par with men in the process of taking security precautions. It is important to include women's experiences and perceptions and to ensure that women are defining security rules and procedures, as well as monitoring and evaluating them.

Ensuring that gender-specific security and protection needs are addressed

As with other security needs, assigning responsibilities for addressing gender-based violence and security risks of women defenders is very important within any defender organisation or group. The individuals responsible for security will ideally have a good understanding of the specific needs of women defenders. It may sometimes be necessary to identify someone else who can bring specific knowledge and understanding to the issue. For example, one person might be in charge of security, but the organisation later decides to appoint a person with the right training and skills to be a focal point for gender-based violence. In such

cases, both people must work closely together to ensure that all security procedures run smoothly and respond to people's different needs.

Training

Training for all those working together in a human rights organisation is key to improving security and protection and should include developing awareness about the specific needs of women defenders.

Awareness raising

- on any confusion between social, cultural, religious values and women rights, human rights.
- on domestic violence against women which includes all physical, sexual and psychological harm occurring within the family, such as battering, marital rape, female genital mutilation and other traditional practices which are harmful and a risk to women's lives.
- within the families of women rights defenders, and the need for taking the same courses of action as they do against the same violence outside the domestic sphere. Organisations should consider any possible contradiction between their aims and members agreeing on domestic violence. From a security point of view, it implies possible discredit to the whole organisation with possible consequent decrease in key stakeholders' support.
- on the fact that many women will be influenced, as far as security is concerned, by the fact that they have to take care of children and other relatives, in addition to their other work. Of how men could promote domestic task sharing without damaging their masculinity.
- on the fact that both women and men human rights defenders are often condemned for dedicating themselves to others instead of to their own families

In summary,

Differences in women's security needs are linked to their different roles, to different kinds of threats, and to differences between specific situations (such as detention, field work, etc.) The aim is to develop gender-sensitive responses to violence against women and other defenders.

Additional comment

Gender-based violence is always **under-reported.** A general awareness about gender-based violence within the organisation or group can make it easier for people to talk about gender specific threats or incidents. Willing staff members can also serve as "entry-points" for women and men defenders who want to find solutions to gender-based threats or violence against them or others in the organisation or community.

Sexual aggression and personal security

Statistically speaking, rape affects more women than men. Some men human rights defenders who have suffered it speak of it as sexual torture and are aware that it is what women go through. Rape is torture in itself as it attempts to the physical and the psychological integrity of a person.

As common law crimes are often a cover when it comes to human rights defenders, for the sake of proportion, one could speak of rape in a real common law crime and one must speak of sexual torture in political crime (repression of defenders' work where victims can either be pre-selected or opportunistic targets).

It is a crime of power and violence. Sexual torture is an alternative way for the aggressor to demonstrate his or her power over the victim.

Sexual torture is one of the consequences of physical aggression. Therefore, prevention needs to start with implementing all security measures described previously to reduce the risk of aggression. This is why, the prevention of sexual aggression might be similar to that of other aggressions.

Remember that in many cases women taken to a different location with a potential aggressor are raped (and beaten or even killed). Thus women should always make a strong and definite decision not to follow the potential aggressor (probably unless such a refusal would severely endanger her life or the life of others

All women rights defenders face the risk of sexual torture but not all women rights defenders are equal in front of it. It depends on the political, social, cultural, religious context. Some women will have to deal with the physical health and psychological consequences others, with the physical health, psychological, social, cultural consequences, the ordeal of reporting it and being questioned about it throughout the legal procedure.

Sexual aggression ought to be approached from all perspectives and consequences, the psychosocial dimension included. Like in all tortures, the sexually tortured person might experience feelings of "lost dignity", distrust, and in case of rape, also being filthy... Organisations might consider the possibility to analyse the concept of dignity: what is dignity? Who decides about the dignity of the other person? Who actually has lost their dignity: the one falling as low as torturing or the tortured?

A permanent organisational policy ought to include:

- mainstreaming women rights defenders specific needs
- tackling organisation gender-discrimination
- considering cultural impact on victims of sexual abuse and torture
- ...

Specific protocols:

- women rights defenders on field missions
- Public relations with stakeholders in protection
- handling consequences of sexual abuse and torture such as unwanted pregnancy and HIV/AIDS.

When defining these protocols do not forget that:

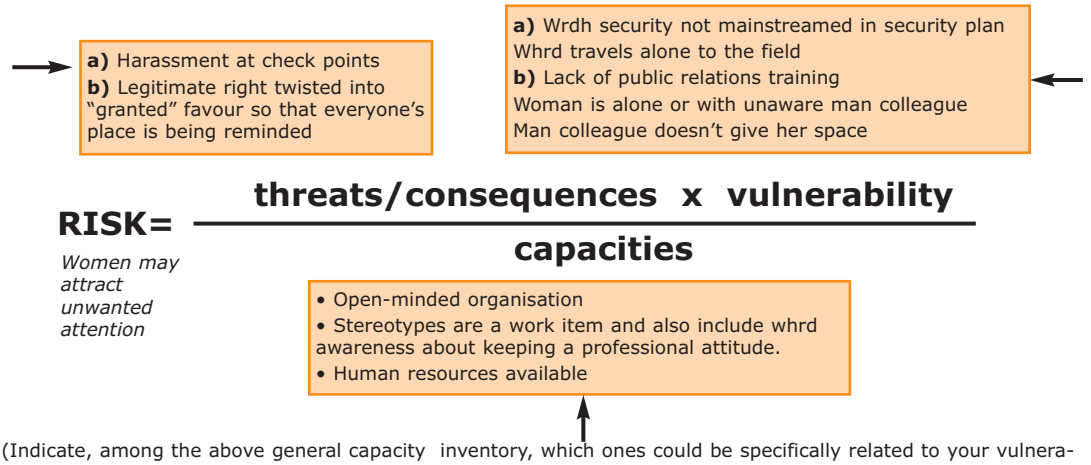
- Some women human rights defenders don't dare to mention that they have experienced sexual abuse and torture with their man peers as they fear stigmatisation
- In some countries mixed organisations hardly ever speak about it.
- Some man human rights defenders have strong opinions on abortion. On the other hand, they are not necessarily ready to foster the unwanted child. In many countries, as abortion is not permitted either by law, culture or religion, infanticide has become a real option alongside with child abandonment. The latter contributing to the witch child phenomenon and the increase in child soldiers, let alone all other social blight. Also, women could consider taking the day-after pill (a pill which will provoke menstruation regardless of the fact that she might or not be pregnant)
- There is no right or wrong choice, there are consequences that ought to be assessed within the organisation.
- **It is important to use the risk assessment tool**

Example:

Risk: *Women may attract unwanted attention.*

List all related possible threats/consequences of the above considered risk. Then, per threat/consequence, list respective current vulnerabilities and capacities. Then determine desirable capacities to reduce vulnerabilities and work on them.

In other words, the risk needs to be unfolded as much as possible, like peeling an onion layer after layer. For each layer (threat/consequence) determine related vulnerabilities and capacities



(Indicate, among the above general capacity inventory, which ones could be specifically related to your vulnerabilities "a" and "b". Then, determine which others you need to develop).

Reacting to a sexual aggression[2]

The options for response to a sexual aggression are just as limited as for all other physical assaults and strictly up to the victim. There is no right or wrong way to react. As all other choices, they imply consequences. In all cases, the primary objective is to survive. The options available to the victim of sexual aggression can include the following:

1 ◆ **Submit.** If the victim fears for his or her life, they may choose to submit to the crime.

2 ◆ **Passive resistance.** Do or say anything distasteful or disgusting to ruin the aggressor's desire for sexual contact. Say you have AIDS (although the aggressor's reaction might be: so what? I have it too, or he could get more violent).

3 ◆ **Active resistance:** Try any type of physical force you can muster to fight off the aggressor r such as striking, kicking, biting, scratching, shouting and running away.

In all cases:

- if possible, try and mention the condom. In some cultures and religions it is falsely considered as "consent" but at the end of the day it is their problem. Yours might be bigger as you might have to live with pregnancy, health consequences and, among all possible recurrent thoughts, also the "what if?"). It means that women human rights defenders might consider keeping condoms on them or wear a feminine condom when in mission to risky areas. It implies talking about it in the organisations and including it in the budget. The same goes for the day- after pill and any hospital treatment (see later: PEP)

- if possible try and gather as much information about the aggressor(s). It might help there and then to concentrate on something and it will definitely help to file the legal case and reduce the probability of impunity.

[2] Most of this information has been adapted from Van Brabant's book *Operational Security in Violent Environments* and from World Vision's and the World Council of Churches' Security Manuals.

- if possible, try and concentrate on mentally separating the body from the soul.

In all cases, do whatever you must to survive. Go with your instincts. No one knows how they will react in such a situation (or any other type of torture) and your way to react will be right for you and the given situation.

In many places, sexual torture takes proportions beyond imagination.
Where basic security logic would suggest not to go to a field mission before having built enough deterrence power as the risk of being sexually tortured by fighting parties is extremely high, some human rights defenders organisations and individual women rights defenders decide to go beyond their own security thinking about the many other victims. Although the line between acceptable and non acceptable risk is personal and organisational, we can't but insist on the basic security rules. During trainings, the brainstorming has gone as far as considering analysing the following options in case of sexual aggression during a field mission: the woman right defender could invoke AIDS (whether it is a collective sexual torture or not) and instil the doubt that as no one knows who might have AIDS, all might be affected. She could also tell the aggressor that she has her periods which means that as a prevention she would need to consider wearing stained sanitary towels during the whole field mission. She could wear more layers of clothes hoping that rescue would come in time.

HIV/AIDS is blight on society and does not have gender barriers.
In some countries where sexual torture of women has become a war weapon, many women are considering meeting with the aggressors and "explain" how it is affecting them all: how the point is not whether to sexually torture women in order to achieve repression rather see that it is leading to collective death: it has become a question of life or death for all, aggressors included. It is a time bomb for all, let alone the cultural genocide.

Many men human rights defenders also work on sexual torture against women and the related cultural rejection. Yet, some of them assert that they would repudiate their wives if it happened to them.

One man human right defender once questioned a male colleague (working on changing family attitude towards sexually tortured women) who considered it as adultery. He simply said to the latter: "it depends on what your wife represents for you".

It is the underlying question. Too often, a woman is considered mainly a sexual object/property: once "broken", drop it and take another one

A woman is often considered a mother, daughter, sister, wife of the man. Hardly as a woman with her own identity. Fortunately, many women can count on their man colleagues who give genuine support to their women peers.

All human rights defender organisations and groups should have preventive and reactive plans in place to deal with sexual aggressions.

Where possible, and depending on the local context and access to medical laboratories, the following should be available:

- medical visit/care before washing – (to take a semen sample or any other sample for DNA analysis)
- pictures of the victim)
- psychological support
- reporting to the competent authority and filing cases.

In all cases, the reactive plan should include, at the very least, providing the victim with **effective healthcare, including psychological care,** followed by legal support (remember that a woman might prefer to be assisted by another woman instead of a man).

To prevent pregnancy, the victim should be offered the day-after pill (within 24 hours): this is an emergency contraception (not an abortive pill).

Although not guaranteed as it depends on many variables, "Post-exposure Prophylaxis (PEP)" can be considered. A post-rape kit is available in some hospitals, containing treatment intended to stop the transmission of several diseases for victims who have managed to receive care within 72 hours of being raped. In any case, check immediately and regularly for sexually transmitted diseases[3]

a careful balance must be achieved between ensuring that the victim has access to the relevant specialist support, and ensuring that the organisation reacts in an appropriate and supportive way.

Please also see *Preventing and reacting to aggressions* in Chapter 1.5.

Summary

Women suffer gender-based abuse, harassment and torture determined by patriarchal culture. Mixed human rights defenders' organisations all too often reproduce it at their micro level. Security for women human rights defenders is security for all human rights defenders.

It needs to be mainstreamed within the security policies and protocols of organisations. More is needed than just a strict risk assessment.
It requires also:

- questioning roles and attitudes
- working on false assumptions and changing gender-driven attitudes.
- positive discrimination to assist changes
- security budget should consider including "condoms, the day-after pill, triple-therapy, ...

Again, there is no guarantee of results. Sexual torture comes after physical aggression. By reducing the exposure to the latter, the probability of sexual torture will also decrease.

[3]More information: International Committee of the Red Cross-ICRC : http://icrc.org/web/eng/siteeng0.nsf/html/congo-kinshasa-feature-201207A

CHAPTER 1.10

Security in armed conflic areas

Purpose:

Reducing the risks inherent in areas of armed conflict.

Risk in conflict situations

Working in conflict areas exposes human rights defenders to specific risks, especially in armed conflict situations: Many of the current killings of civilians are due to indiscriminate-war making practices, and many others are due to the fact than civilians are directly targeted, and we need to recognized this as such. Political action is always needed to highlight this and try to put a halt to it.

Although you cannot exert any control over ongoing military action, you can adapt your behaviour in order to prevent being affected by the conflict or to react appropriately if something happens.

If you are established in an area where armed action occurs regularly, you will probably have developed many of the contacts necessary to protect yourself, your family and the people you work with while you try to continue working.

However, if you are working in an armed conflict area where you are not based, you must **keep three things in mind from the start:**

a ◆ What level of risk are you prepared to accept? This also applies to the individuals/organisation you are working with.

b ◆ Do the benefits of you being in the area outweigh the risks? Long-term human rights work cannot be sustained at the cost of greater exposure to high risk.

c ◆ Simply 'knowing the area' or 'knowing a lot about weapons' will not protect you if you are fired at or come under a mortar or sniper attack.

The risk of coming under fire

Types of fire

You can be exposed to rifle and machine gun fire, mortars, rockets, bombs and missiles from land, air or sea. Fire can be more or less targeted, ranging from a sniper or helicopter in good visibility to directed mortars or artillery barrage. It can also be of the saturation variety, intended to 'pulverise' an entire area.

The more targeted the fire is, the less risk you run - as long as the fire is not directed at you, the general area you are in or a neighbouring area. In such cases the risk diminishes if you can withdraw. **In any event, remember that if you come under fire, it will be difficult to know whether you are being targeted or not. Establishing this is not a priority,** as we shall see below.

Taking precautions: Reducing your vulnerability to fire

1 ◆ **Avoid dangerous places.**

In combat or terrorist action zones, avoid being based, having an office or remaining for long near a possible target of attack, such as a garrison or telecommunications installation. The same applies to strategic areas such as approaches to and exits from urban areas, airports or vantage points controlling the surrounding area.

2 ◆ **Find adequate protection from attack.**

Glass flying from nearby windows is one of the main causes of injury. Boarding up windows or covering them with adhesive tape can reduce the risk of this happening. In case of attack, move away from windows and seek immediate protection on the floor, under a table or preferably in a central room with thick walls, or even better in a basement.

Sandbags can sometimes be useful, but only if other buildings are equipped with them too - otherwise you risk attracting unnecessary attention.

If there is nothing else available, the floor or any depression in the ground can offer at least partial protection.

A simple brick wall or car door will not protect you from rifle or heavier weapons fire. Shelling and rockets can kill at ranges up to several kilometres, so you don't need to be very close to where the fighting is to be hit

Bomb or mortar explosions can damage your ears: Cover them with both hands and open your mouth partially.

Obvious identification of your headquarters, location or vehicles can be useful, but be aware that **this only applies where attackers usually respect your work.** If this is not the case, you will be exposing yourselves unnecessarily. If you wish to identify yourselves, do so with a flag or colours and signals on walls and roof(if there is a risk of air attack).

If you are in a vehicle that is being fired at directly, you can try to evaluate the situation, but making an accurate assessment will be very difficult. In general, **it is useful to assume that the vehicle is or will be a target, and that the correct thing to do, therefore, is to get out and seek cover immediately.** A vehicle is a clear target. It is vulnerable, and exposes you to injuries from flying glass or exploding fuel tanks, in addition to direct fire. If the fire is not too close, try to continue travelling in the vehicle until you can take cover somewhere close at hand.

Landmines and unexploded ordnance (UXO)[1]

Landmines and unexploded ordnance pose a serious threat to civilians in armed conflict areas. They can take different forms:

- **Mines:**
  - Anti-tank mines are laid on roads and tracks and will destroy a normal vehicle.
  - Anti-personnel mines are smaller and can potentially be found in any place where people are supposed to pass through. Most anti-personnel mines are buried in the ground. Do not forget that people planting mines in a road may also mine the fields next to it and smaller paths nearby.
- **Booby traps:**
  - Booby traps are small explosives hidden in an object that looks normal or attractive, (with colours, for example), that explode when touched. The term is also used for mines linked to an object that can be moved or activated (anything from a dead body to an abandoned car).
- **Unexploded ordnance:**
  - This refers to any type of ammunition which has been fired but has not exploded.

Prevention against mines and unexploded ordnance.

The only way to avoid mined areas is to know where they are. If you are not based in or living in the area, you can only establish the location of minefields by continually and actively asking local inhabitants, or experts on the subject, if explosions or combat have occurred in the area. It is better to use asphalted highways, passable roads in regular use, and follow in the tracks made by other vehicles. **Do not leave the highway, not even onto the kerb or hard shoulder, with or without the vehicle.** Mines or other unexploded ordnance can remain hidden and active for years.

2 Much of the information in this section has been adapted from Koenraad van Brabant's excellent manual, *Operational Security Management in Conflict Areas* (see the Bibliography).

Unexploded ordnance can appear in any area where combat or firing has taken place, and can be visible. The golden rule is: **Do not approach it, do not touch it, mark the spot if you can, and make it known immediately.**

Booby traps are normally found in areas which combatants have withdrawn from, In these areas it is imperative to not touch nor move anything and to stay away from abandoned buildings.

If a mine explodes underneath a nearby vehicle or person

There are two golden rules:

- Where there is one mine, there will be more.
- Never act impulsively, even though there may be people with injuries.

If you have to withdraw, retrace your steps if they are visible. If you are travelling in a vehicle and suspect there may be anti-tank mines, abandon the vehicle and withdraw by walking back along the wheel tracks.

If walking towards a victim or withdrawing from a mined area, the only way of doing so is to kneel or lie down and start prodding the ground by sticking a prodder (a very thin piece of wood or metal) carefully into the soil at a 30 degree angle, gently feeling for any hard objects. If you come upon a hard object, clear the side of it very carefully until you can see what it is. Mines can also be triggered by trip wires. Do not cut wires if you find any.

All of this can, of course, take a considerable amount of time[2] .

[2] You can find manuals and resources on mine awareness and education in the Web page of International Campaign to Ban Ladmines: www.icbl.org

CHAPTER 1.11

Security in communication and information technology

(With the collaboration of Privaterra –www.privaterra.org)

Purpose:

The huge gaps in information technology which exist throughout the world also affect human rights defenders. This chapter focuses mainly on information technology – i.e. computers and the internet[1]. Defenders who do not have access to computers or the internet may not find some of the contents relevant now. Instead, they urgently need the necessary means and training to enable them to use information technology in the defence of human rights.

A guide to communication security problems and how to avoid them

Knowledge is power, and by knowing where your potential communication security problems lie, you can feel safer while doing your work. The following list outlines the various ways in which your information or communication can be illegally accessed or manipulated, and suggests ways of avoiding such security problems.

Talking

Information doesn't need to pass through the internet to be illegally accessed. When discussing sensitive issues, consider the following questions:

1 ◆ Do you trust the people you are talking to?

2 ◆ Do they need to know the information you are giving them?

3 ◆ Are you in a safe environment? Bugs or other listening devices are often specifically planted in areas where people assume they are safe, such as private offices, busy streets, home bedrooms and cars.

[1] This chapter is based on work done by Robert Guerra, Katitza Rodr_guez y Caryn Mladen from Privaterra, an NGO which provides courses and consultancy across the globe on security and IT for human rights defenders. Privaterra is currently working on a more detailed manual on electronic communications and security for Front Line which will be published in 2005. (This text has been slightly adapted in some parts by Marie Caraj and Enrique Eguren.)

It may be difficult to know the answer to the third question, because microphones or bugs can be planted in a room to record or transmit everything being said there. Laser microphones can also be directed at windows from great distances to listen to what is being said inside a building. Heavy curtains provide some protection against laser bugs, as does installing double glazed windows. Some secure buildings have two sets of windows installed in offices to reduce the risk of laser listening devices.

What can you do?

- **Always assume someone is listening in.** With an attitude of healthy paranoia, you are more likely to be careful when it comes to confidential matters.

- **Bug sweepers or sniffers can detect listening devices**, but can be expensive and difficult to obtain. Also, sometimes the people hired to conduct the bug sweeps are responsible for the original bugging. During a sweep, they either find a few "throwaways" (cheap bugs designed to be found) or miraculously find nothing and declare your offices "clean".

- **Any cleaning staff could be a serious security threat.** They have after-hours access to your offices and take all your waste away with them every night. All staff should be vetted carefully for security clearance on an ongoing basis, as staff may be compromised after they join your organisation.

- **Change meeting rooms as often as possible.** The more rooms or places you use to discuss and exchange information, the more manpower and equipment will have to be used to listen in.

- **Beware of gifts designed to be kept with you at all times,** such as an expensive pen, lapel pin or broach, or used in your office, such as a beautiful paperweight or large picture. These kinds of objects have been used in the past to listen in on conversations.

- **Assume that some proportion of your information is compromised** at any given time. You may wish to change plans and codes often, giving your listeners only fragments of true information. Consider giving out false information to check if anyone uses or responds to it.

- To minimise laser microphone effectiveness, **discuss delicate matters in a basement or a room with no windows.** Some laser listening devices can be less effective during rainstorms and other atmospheric changes.

- **Play an audio recording of white noise or a popular song** to interfere with sound pick-up as there are also external listening devices that can pick up a conversation within a range of roughly 50 meters. In other words, your meeting place doesn't need to be physically bugged. Only expensive technology can filter out random noise to hear a conversation.

- **Wide open spaces can be both helpful and harmful.** Meeting in a secluded place makes it easy to see if you're being followed or observed, but makes it difficult to escape by blending in. Crowds make it easier to blend in, but far easier to be seen and heard.

- **Should your office or meeting place be in an (open) rural area**, ask one of your members to stay outside and let you know whether they can pick up your conversation and have them watch undesired elements throughout your meeting.

Mobile phones

All phone calls can be listened into if the listener has enough technological capacity. No phone call can be assumed to be secure. Analogue mobile phones are much less secure than digital mobile phones, and both are much less secure than landlines.

Both your location and your conversations can be picked up through cellular surveillance. You don't have to be talking for your location to be tracked – this can be done anytime your mobile phone is switched on.

Do not keep information such as sensitive names and numbers in your phone's memory. If your phone is stolen, this information can be used to track down and implicate people you want to protect.

For emergencies, where possible you might consider getting two unidentified telephone numbers (pay and go phone cards). They can only be used to call each other and never to call or be called by a "known" number (as known number would be on the black list and betray the new number). Don't use them from places that can easily be connected to you. Remember not to leave them on your phone when not needed as they can be tracked down. Change them both regularly. Use the same discretion during conversation as you would from your usual number.

Physical security of information in the office

Keep the office locked at all times, including doors and windows. Use keys that require specific authorisation to be copied and keep track of all copies. Do NOT give keys to third parties, even maintenance and cleaning staff, and make sure you or someone you trust is always present when third parties are in the office. If this is not possible, make sure you have a room with limited access where vulnerable files are kept. Consider locking all office doors and leaving non-confidential waste outside in the hallway at night.

Use a cross-cut shredder for anything confidential. Strip shredders are mostly useless. For disposing of particularly confidential material, consider burning the shreddings, pulverizing the ashes and flushing the ashes down the toilet.

Basic computer and file security[2]

Lock computers away when leaving the office, if possible. Turn computer screens away from the windows.

2 More detailed advice on computer security is available from Front Line by contacting info@frontlinedefenders.org or from Privaterra at info@privaterra.org

Use surge protectors for all power outlets (variations in the electrical current can damage your computer).

Keep back-up information, including paper files, in a secure, separate location. Make sure your back-ups are secure by keeping them on an encrypted computer hard drive with a secure data back-up organisation, or secured by sophisticated physical locks.

To reduce the risk of someone accessing your computer, passphrase-protect your computer and always shut off your computer when you leave it.

Encrypt your files in case someone does access your computer or bypasses your passphrase protection.

If your computer is stolen or destroyed, you will still be able to recover your files if you have created a secure back-up every day. Keep the encrypted back-ups away from your office in a safe place.

You can also use an external server to backup your information on internet. This will allow you recovering all your backed up files even if your computer is stolen or destroyed.

Erased files cannot be reconstructed if you have wiped them using PGP Wipe or another utility, instead of just placing them in the computer's trash or recycle bin.

Your computer can be programmed to send out your files or otherwise make you vulnerable without your knowledge. To avoid this, buy your computer from a trusted source, flatten the computer (i.e. reformat the hard drive) when you first get it, and then only install the software you want. Only allow trusted technicians to service your computer and watch them at all times.

Consider unplugging your computer's phone connection/modem, or otherwise physically disabling your internet connection, when leaving the machine unattended. This way, rogue programs calling out in the middle of the night will not work. Never leave your computer on when you leave for the day. Consider installing software that will disable access after a certain set time of inactivity. This way, your machine is not vulnerable while you get a coffee or make a photocopy.

In your web preferences, enable file extensions in order to tell what kind of file it is before you open it. You don't want to launch a virus by opening an executable file that you thought was a text file. In *Internet Explorer*, go to the *Tools* menu and choose *Folder Options*. Click *View* and make sure the box *Hide extensions for known file types* is NOT checked.

Internet security problems

Your email does not fly directly from your computer to the intended recipient's computer. It goes through several nodes and leaves behind information as it passes. **It can be accessed all along the path (not only in/from your country!)**

Someone could be looking over your shoulder as you type. This is especially problematic in internet cafes. If you are connected to a network, your email may be accessible to everyone else in the office. Your system administrator may have special administrative privileges to access all emails.

Your internet service provider (ISP) has access to your emails, and anyone with influence over your ISP may be able to pressure it into forwarding them copies of all your emails or to stop certain emails from getting through.

As they pass through the internet, your emails flow through hundreds of insecure third-parties. Hackers can access email messages as they pass. The ISP of your intended recipient may also be vulnerable, along with the network and office of your intended recipient.

Basic internet security

Viruses and other problems, such as Trojan Horses or Trojans, can come from anywhere; even friends may unknowingly spread viruses. Use a good anti-virus program and keep up-to-date with automatic online updating. New viruses are constantly being created and discovered, so check out the *Virus Information Library* at www.vil.nai.com for the latest virus protection patches.

Viruses are usually spread through emails, so practice safe emailing (see below). Viruses are single programs designed to replicate and may or may not be malignant. Trojans are programs designed to give a third party (or anyone!) access to your computer.

A good firewall can help you appear invisible to hackers and keep out intruders trying to get into your system. This ensures that only authorised applications can connect to the internet from your computer and prevents programs such as Trojans from sending out information or opening "back doors" to your computer through which hackers can enter.

A "key logger" system can track every keystroke you make. These programs are spread either by someone putting it onto your computer while you are away, or through a virus or Trojan that attacks your system over the internet. Key loggers track your keystrokes and report on your activities, usually over the internet. They can be defeated through passphrase-protecting your computer, practising safe emailing, using an anti-virus program, and using a mouse-guided program to type in your passphrase. Key loggers can also be disabled by physically disconnecting your computer's internet access -usually by simply unplugging the computer's telephone connection - when you are not using the computer.

An email address can be "spoofed" (faked) or used by someone other than the true owner. This can be done by obtaining access to another person's computer and password, by hacking into the service provider, or by using an address that appears to be the specific person's address. For example, by exchanging the lowercase "l" with the number "1", you can create a similar address and most people will not notice the difference. To avoid being fooled by a spoof, use meaningful subject lines and periodically ask questions that only the true person could answer. Confirm any suspicious requests for information by following it up through another form of communication.

Keep your browsing activity private by not accepting cookies and by deleting your cache after every time you use the web. In *Internet Explorer*, go to *Tools*, then *Options*. In *Netscape Navigator*, go to *Edit*, then *Preferences*. While you're in either of these menus, delete all your history, any cookies you may have and empty your cache. Remember to delete all your bookmarks as well. Browsers also keep records of the site you visit in cache files, so find out which files should be deleted on your system.

Upgrade all web browsers to support 128-bit encryption. This will help safeguard any information you want to pass securely over the web, including passwords and other sensitive data submitted on forms. Install the most recent security patches for all software used, especially *Microsoft Office, Microsoft Internet Explorer* and *Netscape*.

Don't use a computer with delicate information stored on it for non-essential web browsing.

Basic safe emailing

These are safe email practices which you and all your friends and associates should follow. Let them know that you will not open their email unless they practice safe emailing.

1 ◆ NEVER open an email from someone you don't know.

2 ◆ NEVER forward an email from someone you don't know, or which originated with someone you don't know. All those "think happy thoughts" emails that people send around could contain viruses. By sending them to your friends and associates you may be infecting their computers. If you like the sentiment enough, retype the message and send it out yourself. If retyping it is not worth your time, it's probably not that important a message.

3 ◆ NEVER download or open an attachment unless you know what it contains and that it is secure. Turn off automatic download options in your email program. Many viruses and Trojans spread themselves as "worms" and modern worms often appear to have been sent by someone you know. Smart worms scan your address book, especially if you use *Microsoft Outlook* or *Outlook Express*, and replicate by masquerading as legitimate attachments from legitimate contacts. PGP signing your emails, both with and without attachments, can greatly reduce confusion over virus-free attachments you send to colleagues (PGP is a software to encrypt information, please see below under "Encryption")

4 ◆ DON'T use HTML, MIME or rich text in your email - only plain text. Enriched emails can contain embedded programs which could allow access or damage your computer files.

5 ◆ If using Outlook or Outlook Express, turn off the preview screen option.

6 ◆ Encrypt your email whenever possible. An unencrypted email is like a postcard that can be read by anyone who sees it or obtains access to it. An encrypted email is like a letter in an envelope inside a safe.

7 ◆ Use meaningful subject lines so the reader knows that you intended to send the message. Tell all your friends and colleagues to always say something personal in the subject line so you know they truly sent the message. Otherwise someone might be spoofing them, or a Trojan might have sent out an infected program to their entire mailing list, including you. However, don't use subject lines that give away secure information in encrypted emails. Remember, the subject line is not encrypted and can give away the nature of the encrypted mail, which can trigger attacks. Many hacking programs now automatically scan and copy email messages with "interesting" subjects such as "report", "confidential" "private" and other indications that the message is of interest.

8 ◆ NEVER send email to a large group listed in the "To" or "CC" lines. Instead, send the message to yourself and include everyone else's name in the "bcc" lines. This is common courtesy as well as good privacy practice. Otherwise, you are sending MY email address to people I don't know, a practice that is rude, offensive and potentially both frustrating and dangerous.

9 ◆ NEVER respond to spam, even to request to be taken off the list. Spam servers send email to vast hoards of addresses and they never know which ones are "live" – meaning that someone is using the email address actively. By responding, the server recognizes you as a "live" account and you are likely to receive even more spam as a result.

10 ◆ If possible, keep a separate computer, not connected to any other, that accepts general emails and contains no data files.

11 ◆ You can also use either two addresses only to communicate between them (as with the example of the two emergency phone numbers and with the same rules). Or, one single address whose mailbox is accessible to more trusted people of your organisation: mails will not need to travel more than once and can be consulted by more. Remember that the more people know about it, the less safe it is. Change the address from time to time.

Encryption: Questions and Answers

The following is a list of frequently asked questions and answers. Feel free to ask us anything else you want to know by contacting the NGO Privaterra through www.privaterra.org

Q: What is encryption?

A: Encryption means scrambling data into a secret code that cannot be deciphered except by the intended party. Given enough time and computing power,

all encrypted messages can be read, but this can take huge amounts of time and resources. In simple terms, encryption is a way for you to secure your files and emails from spying eyes. Your files get translated into code – an apparently random collection of numbers and letters - that makes no sense to anyone who sees it.. To encrypt a file, you "lock" it with a key, represented by a pass phrase. To encrypt a message, you lock it with a key pair using your pass phrase. It can only be opened by the intended recipient, using his or her own pass phrase.

Q: Why should human rights groups use encryption?

A: Everyone should use encryption, because digital communication is inherently unsafe. However, human rights workers are much more at risk than most people and their files and communications are more sensitive. It is imperative for human rights workers to use encryption to protect themselves and the people they are trying to help.

Digital technology is a benefit to human rights groups, allowing them easier communications, greater efficiency and more opportunities. However, with any benefits come certain dangers. Just because you wear a seat belt doesn't mean you are expected to have an accident every time you drive. Driving in a more dangerous situation, such as a race, makes you even more likely to use a seatbelt, just to be safe.

Human rights workers are known targets of surveillance. Since unencrypted emails can be accessed and read by almost anyone, it is almost inevitable that your unencrypted emails will be accessed at some point. Your messages may already be monitored by your opponents and you will never know. The opponents of people you are working to help are also your opponents.

Q: Is it illegal to use encryption?

A: Sometimes. It is perfectly legal to use encryption in most countries of the world. However, there are exceptions. In China, for example, organisations must apply for a permit to use encryption, and any encryption technology on your laptop must be declared as you enter the country. Singapore and Malaysia have laws requiring anyone wishing to use encryption to report their private keys. Similar laws are pending in India. Other exceptions also exist.

The Electronic Privacy Information Center (EPIC) provides an *International Survey of Encryption Policy* discussing the laws in most countries at http://www2.epic.org/reports/crypto2000/. This list was last updated in 2000. If you are concerned check with Privaterra before using encryption in a particular country.

Q: What do we need to keep our IT systems safe?

A: It depends on your system and your activities, but generally everyone should have:

- A firewall;
- Disk encryption;

- Email encryption that also does digital signatures such as PGP;
- Virus detection software;
- Secure back-up: Email all materials to a secure site and do weekly back-ups to CD-RW. Then store it at a separate, secure location;
- Passphrases that can be remembered but not guessed;
- A hierarchy of access – everyone in the organisation does not need access to all files;
- Consistency – none of the tools will work if you don't use them all the time!

But having the right software is not the whole solution. **Individuals are usually the weakest link, not technology.** Encryption doesn't work if individuals don't use it consistently, if they share their passphrases indiscriminately or make them visible, for example, on a sticky note pasted to their monitors. Back-up software won't save you in the event of a fire or raid if you don't keep the back-up copy at a separate, secure location. Sensitive information must be treated on a need-to-know basis instead of being shared with everyone in organisation, so you need to create hierarchies and protocols. In general, it's important to be conscious of privacy and security in your everyday activities. We call this "healthy paranoia".

Q: How do I choose which encryption software to use?

A: Usually, you can ask your friends - and confirm with us. You need to communicate with certain people and groups, so if they are using a specific encryption system, you should use it too to facilitate communications. However, check with us first. Some software packages simply don't do a good job, while others are honey pots. Honey pots lure you into using free and seemingly excellent software provided by the very people who want to spy on you. How better to read your most vulnerable communication than by being the overseer of your encryption software? Still, there are many reputable brands of both proprietary software and freeware - just remember to investigate before you use it[3].

Q: Won't using encryption put me at a greater risk of a crackdown?

A: No one will know you are using encryption unless your email traffic is already being watched. If so, your private information is already being read. That means you are already involved in a crackdown by those doing surveillance on you. There is a concern that those doing surveillance on you will use other options if they can no longer read your emails, so it is important to know your colleagues and implement safe back-up policies and consistent office management at the same time as when you begin to use encryption.

(Note: We have no information from cases in which the use of encryption software has caused problems to defenders. However, consider this possibility carefully before starting encryption, specially if you are in a country with a heavy

[3] For example, PGP –"Pretty Good Privacy"- is a well-known and safe one. You can download it from www.pgpi.org

armed conflict –military intelligence could suspect that you may pass relevant information from the military point of view- or if very few defender use encryption –this could attract unwanted attention on you).

Q: Why do we need to encrypt emails and documents all the time?

A: If you only use encryption for delicate matters, those watching you or your clients can guess when critical activity is taking place, and become more likely to crack down at those times. While they cannot read your encrypted communication, they can tell whether files are encrypted or not. A sudden rise in encryption may trigger a raid, so it is a good idea to start using encryption before special projects begin. In fact, it's best to ensure all communication traffic flows smoothly. Send encrypted emails at regular intervals, even when there is nothing new to report. This way, when you need to send delicate information, it will be less noticeable.

Q: If I've got a firewall, why do I need to encrypt my email?

A: Firewalls prevent hackers from accessing your hard drive and network but, once you send an email into the internet, it is open to the world. You need to protect it before you send it.

Q: No one is breaking into my office, so why should I use privacy software?

A: You don't know if someone is breaking into your system or leaking information. Without encrypted communication, physical security or privacy protocols, anyone can be accessing your files, reading your emails and manipulating your documents without your knowledge. Your open communication can also put others at risk in places where politically motivated raids are more likely to happen. If you lock your doors, you should encrypt your files. It's that simple.

Q: We don't have internet access and have to use an internet café. How can we protect communication sent from an outside computer?

A: You can still encrypt your emails and your files. Before going to the internet café, encrypt any files you intend to email and copy them in encrypted form onto your floppy disk or CD. At the internet café, sign up for an encryption service such as www.hushmail.com or an anonymity service such as www.anonymizer.com, and use these when sending your emails. Make sure the people receiving your communication have signed up for these services too.

Q: If it is that important to secure our files and communication, why doesn't everyone do it?

A: This technology is relatively new, but its usage is spreading. Banks, multinational corporations, news agencies and governments all use encryption, seeing it as a sound investment and a necessary cost of doing business. NGOs are at greater risk than companies, which most governments welcome. NGOs are more

likely targets of surveillance and therefore need to be proactive in implementing the technology. Human rights workers are concerned with protecting persecuted individuals and groups. To do so, they keep files which can identify and locate people. If these files are accessed, these individuals can be killed, tortured, kidnapped, or "persuaded" not to assist the NGO anymore. Information from these files can also be used as evidence against the NGO and their clients in political prosecutions.

Q: One of our principles is openness. We are lobbying for greater government transparency. How can we use privacy technology?

A: Privacy is consistent with openness. If the government wishes to openly request your files, it can do so through proper and recognised procedures. Privacy technology stops people from accessing your information in a clandestine way.

Q: We follow all the privacy and security protocols and our information is still leaked – what's going on?

A: You may have a spy within your organisation or someone who simply cannot keep information confidential. Rework your information hierarchy to ensure fewer people have access to delicate information – and keep an especially watchful eye on those few people. Large corporations and organisations routinely disseminate different bits of false information to specific people as a matter or course. If this false information leaks out, the leak can be tracked directly back to the employee who was given the original, false information.

Dos and don'ts of using encryption

- **DO** use encryption consistently. If you only encrypt sensitive material, anyone monitoring your email traffic will know when something important is about to happen. A sudden increase in use of encryption might lead to a raid.

- **DON'T** put sensitive information in subject lines. They are usually not encrypted, even if the message is.

- **DO** use a pass phrase containing letters, numbers, spacing and punctuation that only you can remember. Some techniques for safe pass phrase creation are using designs on your keyboard or random words strung together with symbols in between. In general, the longer the pass phrase, the stronger it is.

- **DON'T** use a single word, name, popular phrase or an address in your address book for your pass phrase. These can be cracked in minutes.

- **DO** back-up your private key (the file that contents your private key for encryption software) in a single secure place, such as encrypted on a floppy disk or on a tiny, removable "keychain" USB memory device).

- **DON'T** send sensitive material to someone just because they've sent you an encrypted email using a recognisable name. Anyone can "spoof" a name by mak-

ing his or her email address sound like someone you know. Always verify someone's identity before trusting the source – communicate in person, check by phone, or send another email to double-check.

- **DO** teach others to use encryption. The more people are using it, the safer we will all be.

- **DON'T** forget to sign the message as well as encrypting it. You want your recipient to know whether your message has been changed in transit.

- DO encrypt files sent as separate attachments. They are generally not automatically encrypted when you send an encrypted email.

A guide to safer office and information management

Safer Office Management

Safer office management is about creating habits. Office management habits can be useful or harmful. To develop useful office management habits, it helps to understand the reasoning behind them. We've put together lists of habits that can help you manage your information more safely – but only if you develop these habits and think about why they are important.

What is most important for privacy and security in office management?

- Being conscious of your information and who has access to it
- Developing safe habits and using them consistently
- Using the tools properly

Administration

Many organisations have a system administrator or someone who has administrative privileges to access email, network computers and oversee installation of new software. If someone leaves the organisation or is unavailable, the administrator can then access the individual's information and business can continue uninterrupted. Also, this means someone is responsible for ensuring that the system software is clean and from a reputable source.

The problem is that some organisations consider this role merely as technical support and allow a third party contractor to hold administrative privileges. This administrator has effective control over all information in the organisation, and must therefore be absolutely trustworthy. Some organisations share the administrator role between the head of the organisation and another trusted individual.

Some organisations choose to collect PGP private keys and passwords, encrypt and store them securely and remotely with another trusted organisation. This prevents problems if individuals forget their password or lose their private key. However, the location where the files are kept must be absolutely secure and

trustworthy, and specific and extensive protocols must be created relating to accessing the files.

The rules:

1 ◆ NEVER give administrative privileges to a third party contractor. Not only are they less trustworthy than people within the organisation, but someone outside the office may also be difficult to reach in emergencies.

2 ◆ Only the most trustworthy individuals should have administrative privileges.

3 ◆ Determine how much information should be accessible by the administrator: Access to all computers, computer pass phrases, login pass phrases, PGP keys and pass phrases, etc.

4 ◆ If you choose to keep copies of pass phrases and PGP private keys with another organisation, you must develop protocols for access.

5 ◆ If an individual leaves the organisation, his or her individual pass phrases and access codes should be changed immediately.

6 ◆ If someone with administrative privileges leaves the organization, all pass phrases and access codes should be changed immediately.

Software administration

Using pirated software can leave an organisation vulnerable to what we call the "software police". Officials can crack down on an organisation for using illegal software, imposing huge fines and effectively shutting them down. The organisation in question gets little sympathy or support from Western media because this is not seen as an attack on a human rights NGO, but as an attack on piracy. Be extremely careful about your software licenses and do not allow software to be randomly copied by anyone in the office. Pirated software may also be insecure because it can contain viruses. Always use an anti-virus utility whenever software is being installed.

An administrator should have control over new software being installed to ensure that it is checked first. Do not allow installation of potentially insecure software, and only install software that is necessary.

Install the most recent security patches for all software used, especially *Microsoft Office, Microsoft Internet Explorer* and *Netscape*. The biggest threat to security lies within software and hardware delivered with known vulnerabilities. Better yet, consider switching to *Open Source* software, which doesn't rely on the "Security through Obscurity" model, but rather welcomes security experts and hackers alike to rigorously test all code. Using *Open Source* software and any software other than Microsoft has the added benefit of making you less vulnerable to standard viruses and non-specific hackers. Fewer viruses are created for Linux or Macintosh operating systems because most people use Windows. *Outlook* is the most popular email program, and therefore the most popular target for hackers.

Email habits

Email encryption should become a habit. It is easier to remember to encrypt everything than to have a policy of when email should be encrypted and when it should not. Remember, if email is always encrypted, no one watching your traffic will ever know when your communication becomes more significant and delicate.

A few other important points:

- Always save encrypted email in encrypted form. You can always decrypt it again later, but if someone gains access to your computer, it is just as vulnerable as if it had never been encrypted.

- Be persistent with everyone with whom you exchange encrypted emails to make sure they do not decrypt and forward emails, or reply without bothering to encrypt them. Individual laziness is the biggest threat to your communication.

- You might wish to create a few safe email accounts for people in the field that are not generally used and so do not get picked up by spam servers. These addresses should be checked consistently but not used, except by field staff. This way you can destroy email addresses that are getting a lot of spam without endangering your contact base.

General tips for internet cafés and beyond

Emails sent in plain text or unencrypted across the internet can be read by many different parties, if they make the effort to do so. One of these may be your local Internet Service Provider (ISP) or any ISP through which your emails pass. An email travels through many computers to get from the sender to the recipient; it ignores geopolitical boundaries and may pass through another country's servers even if you are sending emails within the same country.

Some general tips on issues commonly misunderstood by internet users:

- Password-protecting a file does so little to protect the file that it is not worth doing for documents containing sensitive information. It only provides a false sense of security.

- Zipping a file does not protect it from anyone wanting to see what is inside.

- If you want to make sure a file or email is sent securely, use encryption (see www.privaterra.com).

- If you want to send an email or a document securely, use encryption all the way to the final recipient. It is not good enough to send an encrypted email from a field office to New York or London or anywhere else and then have that same email forwarded unencrypted to another person.

- The internet is global in nature. There is no difference between sending an email between two offices in Manhattan and sending an email from an internet café in South Africa to a London office computer.

- Use encryption as often as possible, even if the email or data you are sending are not sensitive!

- Make sure the computer you are using has virus protection software. Many viruses are written to extract information from your computer, whether it be your hard drive contents or you email files, including email address books.

- Make sure your software is properly licensed. If you are using unlicensed software, you instantly become a software pirate instead of a human rights activist in the eyes of governments and media. The best option is to use open source software – it's free!

- There is no 100% secure solution if you are using the internet. Be aware that a person can "socially hack" into a system by pretending to be someone they are not on the phone or by email. Use your own judgement and common sense.

Summary

Remember that the parties interested in your work have not waited for technologies to try and get information from you.

Many human rights defenders are reluctant in using secure information technology. Yet, basic procedures are simple.

Basic simple procedures are: discretion in phone and face to face communication, pgp in email communication and for sensitive files, passwords to access your computer.

But having the right software is not the whole solution. **Individuals are usually the weakest link, not technology.**

PART II

ORGANISATIONAL SECURITY

In second part of this Manual we are covering security at organisational level, that is to say ways of improving security within defenders' organisations.

Security/protection does not simply mean having a security plan.

It requires ownership of the whole process, starting with improving the original organisational level of security, to implementing it, and later to managing the improvement process itself.

Acquiring ownership of the whole process is part of the security itself.

The organisational security process is pragmatic and inclusive.

It needs to be realistic and appropriate to the profile of the organisation.

Although it will require resources, changing behaviour is free and constitutes a crucial factor in improving security.

CONTENTS OF SECOND PART:

CHAPTER 2.1

Assessing organisational security performance: the security wheel

Purpose:

Assessing your way of managing security.

Evaluating the extent to which security is integrated into human rights defenders' work.

In order to achieve this, we suggest a two-fold approach:

- Self assessment by the organisation of its security performance: the organisation looks at its own security performance by gathering objective information. The self assessment process can be collective and/or individual. It is interesting to actually see how the members of a same organisation can reach different conclusions about the security performance of the whole organisation.

- How 'others' perceive the organisation

ORGANISATIONAL SELF ASSESSMENT OF SECURITY

The security wheel

The organisational self assessment can objectively be conducted by implementing the security wheel and its eight spokes.

A wheel must be round to turn; in other words, all the spokes need to be the same length.

The same applies to the security wheel and its 8 spokes (components) representing the security management in an organisation or group of defenders.

This assessment can be done in groups:

- sketch out the wheel
- fill in each spoke according to how developed you think it is
- list reasons (brainstorming)why specific spokes are less developed; as all spokes must be at least as long as the most developed spoke, suggest

ways of achieving that result: set objectives and relevant processes, anticipate possible problems and suggests solutions.

- Once you have completed this exercise, keep your security wheel and repeat the exercise a few months later. You will be able to compare both wheels and determine point by point whether things have improved.

The 8 spokes (components) of the security wheel

Acquired security experience and cohesion: practical and shared knowledge of security and protection, gathered through work. The starting and the ending points of the assessment.

Security training. Security training through courses or through individuals' own initiative during daily work.

Security awareness and attitude: Relates to whether individuals and the whole organisation really view protection and security as necessities and are prepared to work towards ensuring it.

Security planning: planning security and protection into your work.

Assignment of responsibilities: who is responsible for what aspect of security and protection? And what happens in cases of emergencies?

Degree of ownership of security rules / compliance: to what extent do people respect security rules and procedures?

Analysing and reacting to security incidents: to what extent are security incidents being analysed? Is the organisation's response adequate?

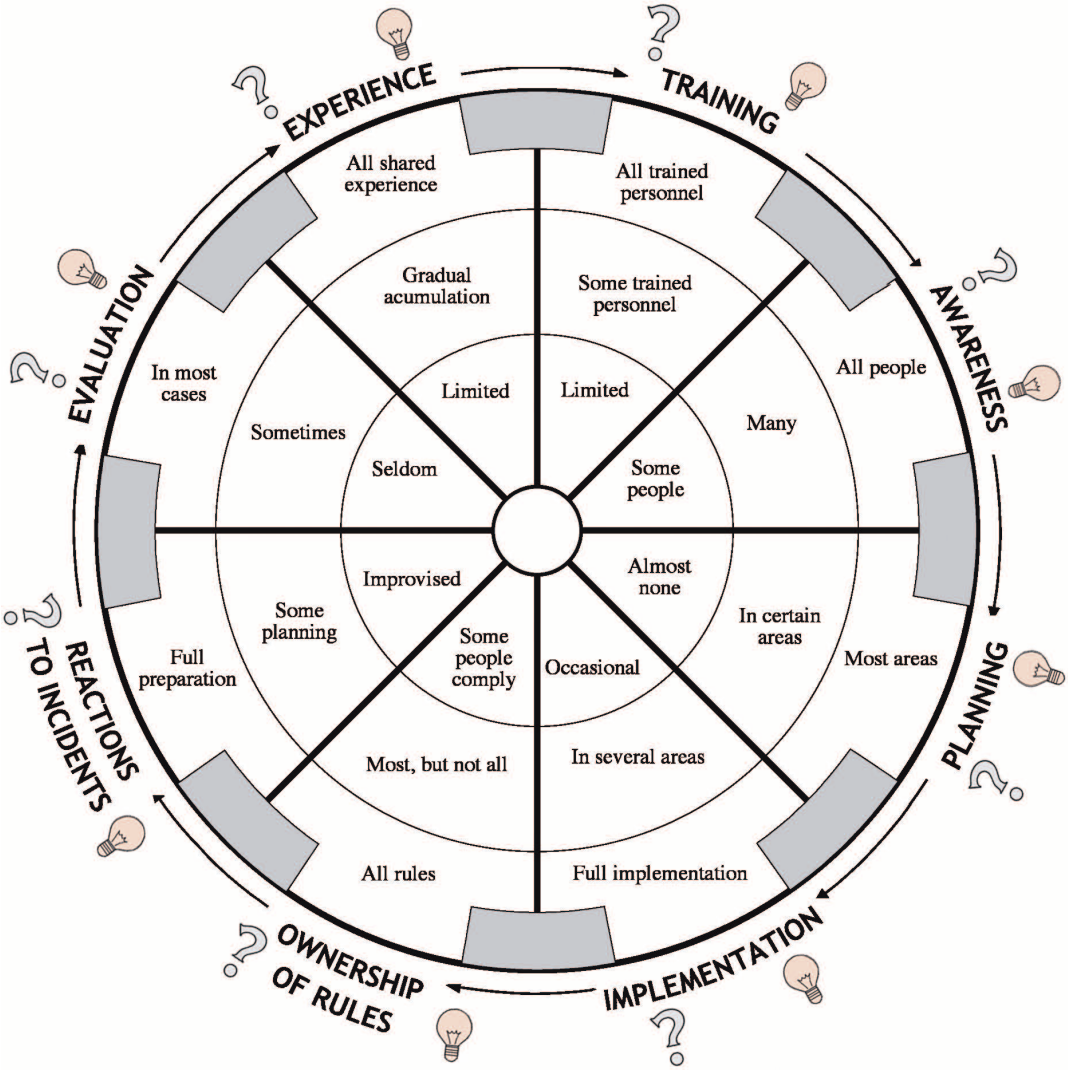
Evaluating security and protection management: to what extent does the organisation evaluate its security and protection management and to what extent is it updated?

Here is a sample security wheel:

The security wheel is never perfect: Some components are more developed than others. It is therefore more useful to determine the degree of development of each component. In this way, you can identify which types of action need prioritising in order to improve your protection and security. The dotted lines going from the centre to the outside edge illustrate how developed this component of the wheel is.

Possible problems related to this part of the wheel...

...and possible solutions to the problems.



Photocopy the wheel onto paper or acetate and add colour to the gaps between the spokes to illustrate visually the actual shape of the wheel for your group or organization. You will then easily be able to see which components are more - and less - developed.

Step by step analysis of the "security wheel"

A proper assessment of the security policy of an organisation requires time to examine the actual meaning of every single component of the security wheel.

1 • Security experience and cohesion acquired through work experience and sharing:

Accumulated practical knowledge and cohesion of security and protection. The start and end points of the assessment.

Bear in mind that the experience of just a few members does not equate to the experience of security at the organisational level but rather to the total of the experience of all its members: sharing experiences will therefore contribute to security cohesion.

The total knowledge will be reflected in the spokes; once you have developed all the components to your satisfaction, the total knowledge will have grown further as a result. Security knowledge will then probably be better developed and all the other spokes will need to follow suit. It is a never-ending activity for the simple reason that organisation members come and go, the political context changes and so does security. However, the good news is that as it is the result of all the other 7 spokes, for this specific spoke you do not need to do anything (unlike for the other 7 ones).

2 • Security training.

Indicate the security training you have had either through a course, or through your own initiative during your daily work.

Questions needing further development :

Are security training procedures available to everyone ? Do we upgrade them? Are new staff members trained? What difficulties would we encounter if we were to train everyone? What are the possible solutions?

3 • Raising security awareness and proper attitudes.

Questions used to determine the current level of awareness:

Is everybody truly aware of security and protection? How could we achieve it?

Awareness does not mean compliance (for example, smokers know how dangerous smoking can be and yet they keep smoking)

Questions to raise awareness:

What factors trigger revision of the security?

What are the stories that are told and what is the informal knowledge of security in the organisation?

What problems would we encounter in raising awareness? What are the possible solutions?

4 ● Security planning:

Questions to determine the current level of security planning:

- Do we plan security and protection into your work?
- Is the security issue integrated (mainstreamed) into the whole institutional approach? (mission, strategic plans, areas of work, transverse themes) ?
- Is security an agenda item within most major meetings (and not the last item on the list)?
- What is the budget strategy (is it ad hoc for security, or is it included in other strategies?) and financial management?
- Do we carry out an analysis of the work environment -in working groups- (at local, regional and national level)?

Do we:

- analyse the impact of the work and how the organisation is perceived by actors that might be pose a threat.
- carry out a full risk analysis: threats, vulnerabilities and capacities
- compile all security documents: review their content and see how they are used
- draft and update security documents: check whether they are up to date and how this can be achieved. - check whether the impact of the work and risk factors have been taken into account. Check if there are processes in place for daily consultation on security.

Do we have security schemes that are:

- simple and clear? Do they contain the necessary information in clear wording?
- drawn up in cooperation with all the people affected?
- appropriate to every work context?
- improved, developed and updated thanks to the initiative of different people of the working group?
- genuine and adapted to the "real world"?

Do our security schemes cover:

- all necessary items?

- communication, IT and information management?
- personnel management (including recruitment)? stress management?

Is everyone aware that a working group with a good structure, good internal communication flow, good public relations and good cooperation is a basic security requisite?

Questions aimed at further developing security planning:

What problems would we meet if we tried to tackle each of the above items?

What could be the solutions?

5 ● Assignment of responsibilities:

Questions to determine the current level of assignment of security responsibilities:

- do we clearly know who is responsible for what aspect of security and protection? And in the event of emergencies?
- Are there organisational responsibilities and duties on workers and collaborators (including their behaviour away from work and family)?
- Does everyone take on their responsibility for security and are there specific responsibilities for different aspects of security? (What difficulties do we encounter?)

Questions to improve assignment of security responsibilities:

What problems would we meet if we wanted assign and share security responsibilities?

What could be the solutions?

Assigning responsibilities contributes to sharing security.

6 ● Degree of ownership of security rules / compliance:

Questions to determine the current level of ownership of security rules / compliance:

- To what extent do people respect security rules and procedures?
- To what extent do each individual and the whole group contribute to the security plan drafting, and comply with the protection and security rules?
- Can we tell if security rules are not being followed, and if not, why not?
- Do people abide by security rules out of fear of reproach or because they are convinced that following the security rules will decrease the

consequences of risks? (e.g. a driver may wear their safety belt either out of fear of a fine or because they are convinced that it will decrease the consequences of a possible car crash)

Questions to improve degree of ownership of security rules/ compliance:

What problems would we encounter in improving the level of respect of the rules?

What are the possible solutions?

7 • Security incident analysis and reactions.

Questions used to determine the current level of security incident analysis and reactions:

- to what extent are security incidents being analysed and do they generate an adequate feedback from the organisation? What security incidents occurred? How were they handled and what damage was caused?
- do we write reports (and how)?
- do we carry out analyses (how and at what level)?
- what is the feedback (deadlines, feedback procedure, responsibilities)?
- how do we evaluate the feedback?
- is training within the organisation based on the incidents (is it done at all? are there institutional channels for this?)
- in short, what is done with the incidents?
- is there a procedure for collecting, investigating, and analysing the security incidents to create a feedback and a basis for our strategies and our plans? are the conclusions mainstreamed into our work and evaluations (where necessary)?
- are there clear plans and responsibilities covering reactions in case of emergencies?
- to what types of emergency are they applicable?

Questions to improve security incident analysis and reactions:

What are the problems for improving every item listed above?

What are the possible solutions?

8 • Assessing security and protection management:

Questions to determine the current level of assessment of security and protection management:

- to what extent does the organisation evaluate its security and protection management and to what extent is it updated?
- is the assessment an institutionalised activity?
- are we aware that day to day work and reactions in the event of security incidents need to be assessed from a security standpoint so that they will contribute to the knowledge and experience of every single person and of the whole organisation?

Questions aiming to improve the assessment of security and protection management?

What problems would we encounter in improving the assessment of security and protection management.

What are the possible solutions?

HOW 'OTHERS' PERCEIVE THE ORGANISATION

Security and our image

It is important to look at the environment of the organisation to see how its organisational image is perceived and whether it corresponds to the image the organisation seeks to convey. It is also important to find out how others perceive the protection and security of the organisation. This should be done from the following points of view:

- from the point of view of the people with whom we work: counterparts beneficiaries,
- colleagues and similar organisations
- financing institutions and sponsors (some may be more receptive than others)
- authorities with which we are in relation
- other actors who might be potential aggressor
- ...

It is also important to ascertain what level of security cooperation there is with other organisations or networks, with counterparts, with people with whom we work, etc.

Here are two non-exhaustive lists of useful thematic questions:

I ◆ Organisational image and impact of the organisation work. How can we assess it?

- How do we learn about our organisational image?

- How to explain it to others?
- What is the purpose of the organisation?
- What are our activities?
- How do our activities affect armed actors or others?
- What capacities or power do we have to keep our work space open?
- What do we do to keep it open?
- How do we think our potential aggressor perceives us?
- Are we perceived as an organisation that handles well its work-related protection and security issues?
- Is there anybody who singles out our work or our handling of it from a security standpoint? Why? How can we tell?

II ◆ Organisational image and impact of the organisation work. How are we perceived?

Try to answer the following questions about us from the point of view of the 'enquiring' party of your: (repeat the exercise for as many parties as you deem necessary: "they' is you and "we" is the enquiring party)

- Who are they?
- What do they expect?
- What is their work?
- How do they hinder our work? What are the limits to our work?
- What can we do? How can we protect ourselves?
- How can we obtain what we want?

Once you have assessed the perception of others you need to see how you could change your image if it does not suit you. Not all perceptions can be changed, of course. But it helps to be aware of them has they may have an impact on your security and protection.

Summary

To assess your security you need a two-fold approach:

Self- assessment (a look at yourself) and assessment of how others perceive you.

Self-assessment can be achieved through the security wheel with its 8 spokes.

It is a snapshot of your current level of security and protection.

It allows development of each spoke so as to achieve a round wheel.

To develop your security wheel you need to start with an inventory of your current situation, set objectives and decide on relevant improvement processes. Try to anticipate possible obstacles during the progress towards your objectives. Try to anticipate solutions.

An assessment of how others perceive you can be achieved by trying to imagine how they would be talking about you.

Of course, you can also put the questions to trusted parties .

You need to find ways of changing any perception that does not suit you. Not all perceptions can be changed, of course. But it helps to be aware of them has they may have an impact on your security and protection.

CHAPTER 2.2

Making sure security rules and procedures are followed

Purpose:

To think about what makes members and organisations unable or unwilling to follow security plans and procedures, and find appropriate solutions.

Security is everybody's business

Whether people and organisations actually follow security procedures and rules is a complex issue. It is quite possible to have a good security plan, complete with preventive rules and emergency procedures, and have security placed high on agenda at all major meetings, etc, and yet have people still not complying with the organisation's security rules.

This may sound incredible, given that human rights defenders are constantly under pressure and threats, but it does happen.

If someone wants to know something about your work, they will not try to find out from the most careful person in the organisation. Rather, they will try to get close to someone who often gets drunk on Saturday nights. Similarly, if someone wants to give your organisation a fright, they probably will not assault a person who has taken all the necessary precautions. Rather, they will probably target someone who is usually quite careless about their own security. Similarly, it could be that a careful person is attacked because the careless person left the door open… The point is that one person's carelessness can place everyone at greater risk. Security is only as good as the weakest of its underlying elements -in this case to the negligence of one individual.

This is why security should be defined as an issue for the whole organisation, as well as for the individuals it involves. If only three out of 12 people follow the security rules, the whole organisation, including those who observe the rules, is put at risk. If the situation improves and nine people start following security procedures, the risk is reduced. But the risk would be smaller still if all 12 people followed the rules.

Security is an issue for the whole organisation, as well as for the individuals it involves.

Having a good security plan is meaningless unless it is being followed. Let's be realistic: many people do not follow rules or procedures. The lack of compliance amounts to the difference between good intentions and actual practice. It is nevertheless easier to confront this problem than its possible consequences.

Why do people fail to follow security rules, and how can we avoid this from the outset?

First of all, the word "compliance" carries connotations of submissiveness and docility and should therefore be avoided. People only follow rules that they understand and accept, because they can then make them their own. Therefore, the key word here is "ownership".

In order for a security procedure to be followed, everyone in the organisation has to embrace it. This doesn't happen instantly. In order for group members to embrace a security procedure they must be allowed to participate in drawing it up and implementing it. Training, understanding and acceptance of the procedure are also crucial.

Table 1: The relationship between individuals and organisations in security terms

Concept	Approach: "Everyone must follow the rules!"	Approach: "The individual and the organisation have agreed on the rules!"
Approach	Rule-focused	Based on organisational and personal security needs
Type of relationship between the individual and the organisation	Normative or "paternalistic"	Based on dialogue
Why do we follow the rules?	By obligation, to avoid sanction or expulsion	To observe an agreement, with room for criticism and improvement (ownership and persuasion is achieved when we are convinced that it fits our needs and it will decrease the feasibility and consequences of a risk and it will contribute to protect our colleagues and the people we work with/for)
Responsibility for security	Not shared	Shared

Ownership is not just about "following rules", but about establishing an agreement about the rules that will make individuals follow them because they understand them, see them as appropriate and effective, and feel they have a person-

al stake in them. For this reason, the rules should also conform to individuals' moral and ethical criteria and basic needs.

Ownership is not about simply "following rules", but about respecting an agreement between the organisation and group members regarding security.

In order to maintain the agreement between group members and the organisation it is important that **the individual(s) responsible for security** should **keep others constantly involved** through briefings, reminders about aspects of the agreement, and by asking people's opinions on how appropriate and effective the rules are in practice.

Such involvement will however be of little value without an **organisational culture of security** which underpins formal and informal work procedures or programmes.

In summary, the necessary basis for people to observe security rules and procedures can be achieved through the following steps:

- Developing an understanding that security is important for the protection of victims, witnesses, family members and colleagues, to enable the core work of the organisation to continue;
- Developing and valuing an organisational security culture
- Creating ownership of security rules and procedures;
- Making sure all group members participate in designing and improving security rules and procedures;
- Training people in security issues;
- Making sure all group members are convinced of the appropriateness and effectiveness of security rules and procedures;
- Drawing up and concluding an agreement between the organisation and individuals about respecting security rules and procedures;
- Involving those responsible for security in briefing and training people, in reminding group members of the terms of the agreement and in asking their opinions on how appropriate and effective the rules are in practice.

Why security rules and procedures are not followed

There is no prototype of a human rights defender who doesn't follow security rules. Many people within an organisation often follow some rules but not others, or observe the rules sporadically.

There are many possible reasons why people don't observe the rules and procedures. To change this and ensure ownership, it is important to establish the causes and find solutions alongside the other people concerned. It will also be useful to distinguish between the different reasons people may have to not follow the rules, because they will vary.

Some possible reasons for not observing security rules and procedures:

Unintentional:

- The defender is unaware of the rules;
- S/he doesn't apply the rules properly.

Intentional:

General problems:

- The rules are too complicated and difficult to follow;
- The procedures aren't within easy reach in the office or are presented in a way that makes them difficult to use day-to-day.

Individual problems:

- The rules are at odds with the individual's needs or interests and this conflict hasn't been resolved;
- The individual does not agree with some or all of the rules and considers them unnecessary, inappropriate or ineffective based on personal experience, previous information or training or because of personal beliefs.

Group problems:

- Most group members don't follow the rules, or group 'leaders' either don't follow them or don't do so enough, because there is no organisational security culture;
- A general lack of motivation at work can lead people to ignore security rules.

Organisational problems:

- There aren't sufficient financial or technical resources to make it easy for group members to follow the rules;
- There's a contradiction between the rules and particular areas of work. For example, rules have been established by those in charge of security but ignored or not properly implemented by people working in programmes or accounts. Some rules might suit one work area and contradict another;
- Group members and staff have a heavy workload and limited time, and don't prioritise some or all of the rules;
- A general lack of motivation, arising as a result of stress, workplace disputes, etc.

Organisational culture is both formal and informal, and must be developed not just in the organisation as a whole, but also in teams. A good organisational culture will be revealed in signs such as informal chatting, joking, parties, etc.

Monitoring the observance of security rules and procedures

Direct monitoring:

Security rules and procedures can be incorporated in general work appraisals and "check-lists"; as well as in meetings before and after field missions, in work reports, on meeting agendas, etc.

Periodical reviews can also be carried out together with the teams in question, of issues such as the safe-keeping of sensitive information, copies and security manuals; of security protocols for visits to the organisation's headquarters; preparing to go on field missions, and so on.

Indirect monitoring:

Asking people for their views about rules and procedures, whether they are appropriate and easy to follow, etc, can establish whether the group members actually knows the rules, whether they have been fully accepted or if there is some disagreement which should be dealt with.

Group members usage of the security manual and any existing protocols and rules can also be reviewed.

It is worthwhile to compile and analyse, along with the people or teams in question, people's opinions and evaluations of security rules and procedures. This can also be done off the record/anonymously or via a third party.

Retrospective monitoring:

Security can be reviewed by analysing security incidents as they arise. This must be handled especially carefully. Someone who has experienced a security incident might worry that it was their fault and/or that analysis will lead to sanctions against them. S/he might therefore be tempted to conceal it, leaving the incident, or aspects of it, unreported.

Who does the monitoring?

Depending on the way the organisation operates, whoever is responsible for organising security, specific areas of work within security and managing any security group members, will also be in charge of monitoring security.

What can we do if security rules and procedures aren't being followed?

1 ◆ Establish the causes, find solutions and put them into practice. The list of options in Table 1 above can be used as a guide.

2 ◆ If the problem is intentional and only involves one individual, try to

- a • engage in a dialogue with the person to establish the cause(s) or motive;
- b • work with the individual's whole team (this can sometimes be inappropriate, depending on the case);

c • apply a notice or warning system, so that the person is fully aware of the problem;

d • use a system of gradual sanctions which could culminate in the person being sacked.

3 ◆ Include a clause about observing security rules and procedures in all work contracts, in order for all staff to be fully aware of how important this is to the organisation.

In conclusion...

Some may argue that a discussion of the reasons why people don't follow security rules is a waste of time, as there are more urgent or important things to be done. Those of that opinion usually believe that rules are simply there to be followed, full stop. Others are aware that the world doesn't always work that way.

Whatever your opinion, we now invite you to step back and analyse the degree to which security rules and procedures are being followed in the organisation(s) where you work. The results could be surprising and worth spending time on, in order to avoid problems further down the line…

Summary

Security is everybody's business

Security is an issue for the whole organisation, as well as for the individuals it involves.

The reasons why people do not follow security rules need to established; they may be:

- unintentional (individual problem)
- intentional (general, individual, group, organisational problems)

Knowing them will contribute to finding appropriate ways to handle then. However, monitoring through an appointed body is recommended (direct , indirect and retrospective monitoring).

Developing an organisational culture of security is fundamental

CHAPTER 2.3

Managing organisational shift towards an improve security policy

Purpose:

To learn how to manage organisational shift towards an improved security policy.

Steps and issues around which the process will be built:

- improving management of the security strategy
- improving the security management implementation process
- what is the entry point? What body is responsible for it? What is the starting point? How to proceed? What about the implementation? What are the pros and cons? What are the obstacles?

Handling security challenges: step by step security management

Security management never ends and is always pragmatic, partial and selective. This is because:

- There are limits to the amount of information you can deal with - not all factors affecting security can be grouped and treated simultaneously;
- It is a complex process - time and effort are necessary to create awareness, develop consensus, train people, deal with staff turnover, implement activities, etc.

Security management can rarely attempt a comprehensive, long-term overview. Its contribution lies in the ability to prevent attacks and highlight the need for organisational strategies to cope with these. This may not seem very ambitious, but we must not forget that often too few resources are allocated for security!

When reviewing a defender's or an organisation's security practices, you may find that some sort of guidelines, plans, measures or patterns of behaviour are already in place. Conflicting forces will be involved, ranging from stereotypical ideas about security practices to a reluctance to increase existing workloads by incorporating new security activities.

Security practice is typically a fragmented and intuitive work in progress. Security management should aim to make step-by-step changes to improve performance. Security rules and procedures tend to emerge from the parts of an organisation covering specific areas of work, such as logistics, a field team especially concerned with its security, or a manager under pressure by donor concerns about security, etc.

Step-by-step security management opens the door to informal processes and allows space for new practices to take root. Sudden events, such as security incidents, will prompt urgent, short-term decisions that, if properly managed, will shape longer-term security practices for the whole organisation.

Security strategy improvement: possible entry points.

Once the need for improving security has been established, it needs to be promoted. There are several entry points for it (either in or outside the organisation):

Inside the organisation:

- management, board of directors or leaders
- intermediate/ executive level
- staff, rank and file
- a combination of all above possibilities.

Outside the organisation:

- donors
- partners, counterparts
- similar organisations working in the same network.

Let's compare their advantages and disadvantages.

Possible entry points to promote the necessity of changes?	Advantages	Disadvantages	Possible Solutions
Entry points **inside** the organisation			
Management, board of directors or leaders	• Can call meetings or general assemblies • Have historical memory • Moral authority • Institutional support • ...	• Perceived as 'imposing security' and generate disinterest- make it too formal, rigid, distant be patronising • See security as an issue affecting them only • Dismiss it as not a priority • ...	• Meetings or general assemblies • ...

INTERMEDIATE/ EXECUTIVE LEVEL	• A view on the upper and lower levels • Easy access to both other levels • Convivial communication channel between both levels. • Communication • Technical capacities to implement security changes • ...	• Often this level does not exist • Partial focus: on one side or area only • Distracted by personal career interests • "Too" technical if not involved in political and field activities • ...	• Involvement procedures (both towards directors and towards members in general • ...
STAFF, RANK AND FILE • **...**	• Can mobilise people • Aware of the mechanisms and details of everyday work • ...	• Might have problems with managers or with hierarchy • ...	• In general, with the group as a whole, acknowledge the problem, the need for everyone's input and the need for solutions. Then, delegate solution-finding to a working group • ...
ENTRY POINTS FROM **OUTSIDE** THE ORGANISATION			
DONORS, PARENT ORGANISATIONS, •...	• More distance • No direct interests. • May have more comprehensive experience • Could call meetings with any and all the above levels without conflicts of interest. • ...	• May have credibility problems or little knowledge of the work that is being done. • Approach might be "too" technical and technical approach • ...	Point out common interest in security Donor organisation prefers to invest in an organisation taking care of security rather than risking losing its investment in an organisation that disregards security Inter-organisational security depends on common security attitudes and rules • ...

The entrance process can be implemented by all organisations, regardless of their size, stability, location.

Which is the body responsible for the improvement process?

Now that that entry has been gained (the need has been promoted and acknowledged), some part of the organisation has to lead the process. Which body will be made responsible for the security improvement process? There are several possibilities:

- Ad hoc members of the organisation (they are part of the organisation and are chosen by it (usually they also have other responsibilities). It can also be a working group (made of people from various areas of work)
- An outside-inside person: a person partially involved in the work and who interacts closely and continuously with the people from the organisation (for example, a person who used to work for the organisation).
- A consultant or adviser: interacts with the ad hoc security person or with the working group (a short-term interaction).

Let us examine the advantages and disadvantages of these different approaches.

Body responsible for the improvement process	Advantages	Disadvantages	Possible Solutions
Ad hoc person from the institution	• Centralised information • Easy access to information • Clarity in terms of responsibility • Easy decision-making - fewer people involved • Chosen for their skills • ...	• Work overload - weakened collective commitment • Excessive dependence on one person • Possible lack of feedback on plans and ideas. • ...	• Distinction between promotion/coordination and implementation • Temporary workload reduction to enable the focus on security. • Support personnel • Constant circulation of strategies so as to ensure progressive feedback • ...
Working group	• Sharing and comprehensive approach of the work on security • Extensive and diverse experience- • More human resources • Distribution of responsibilities: more clarity for initiative and activity. • higher probability for protocols to be followed. • ...	• Work overload • Slow consensus building when taking decisions • Circulation of information less fluid -higher number of persons to be trained for the task. • ...	• Adequate distribution of skills and duties • Involvement of the management level • Rotation, training and commitment to proactive progressive circulation of output in construction in order to get feedback and share the process. • ...
An outside-inside person	• Larger objectivity in risk analysis • Skilled person, trusted by the organisation • Full commitment • Proven receptivity -awareness of strengths and weaknesses • ...	• Discontinuity • May weaken the group commitment • May undermine the due ownership of the whole process and topic. • ...	• Train 1 or 2 team members • Continuous circulation of output in progress and feedback from the whole team • Consensus building and agreements • ...
Consultant or advisor	• Can train the team • Specialised consultancy • Clarity in monitoring the process • Recognised advice • Active follow-up process • Less affected by internal organisational issues • ...	• Can generate dependency instead of skills • Can be seen as “someone there to do the work” instead of “someone there to ease the work” • May undermine the due trust within the organisation • Increased costs • Consultants in this field are rare • Difficulties in organising the work schedule • Might have insufficient knowledge of the context • Might produce a plan and rules inappropriate for the work context • ...	• Clarify as much as possible with everybody: explain the consultant’s role, scope. • Raise the importance of security with other agencies in order to tackle and share the issue • Hold security training of trainers in organisations and institutions (facilitators) • Briefing on work context • …

What is the starting point of the process?

Now that entry has been gained and the responsible body has been appointed, where can the latter start from?

The starting point ought to be the evaluation of the whole-organisation security policy implementation process. Starting from the evaluation (or diagnostics) will determine the priorities and the possible solutions (best practices according to the stated needs, organisation profile and mandate). A plan will then be drawn up aiming to structure the improvement process. The plan will include intermediate goals in order to monitor whether and how progress is achieved. In addition, the plan will clarify the role and responsibilities both of the person/people in charge of the process and of the organisation members. The plan will also include a schedule. At the end of the planned process, an evaluation of achievements will take place.

Diagnostics ⇨ priorities ⇨ possible solutions
⇨ improvement plan ⇨ evaluation

Once priorities are determined, the decision about their order of implementation might be easier if criteria are set: emergency, current available resources, etc

Flexibility is an essential factor throughout the process. However, what it is the minimum needed in order for the improvement process to have a genuine opportunity to achieve positive results? Answering this question before the process starts is crucial.

Diagnostics and improvement plan.

The diagnostics can be carried out using can use the "risk assessment" and the "security wheel" tools, described in previous chapters of this manual (any organisational review methodology can also be useful for this).

It is well known that this step should involve all concerned people and work teams within the organisation.

The improvement plan has to be **realistic** and **appropriate** to the profile and needs of the organisation. Here is a possible sequence of steps:

1 ◆ Identify the organisation's expectations and expected outcomes of the security improvement plan.

2 ◆ Diagnose together, reach a consensus and share ideas about the current structure of security management (application of the "risk analysis" and "security wheel"): Indicate the progress, shortages and needs.

3 ◆ Indicate and discuss the best practices to be implemented in tackling the shortages and needs revealed.

4 ◆ Indicate the desirable and desired objectives of the improvement plan.

5 ◆ Outline the activities required to reach those objectives and what can reasonably be expected for each activity (this will enable progress towards the objectives)

6 ◆ Outline the necessary resources (financial, human, time, technical resources). Define the responsibilities and work schedule.

7 ◆ Define what risks arise from achieving these objectives and outcomes.

8 ◆ Define indicators for monitoring progress and final results.

9 ◆ Share the plan with all the involved parties in order to get feedback, to improve it and to generate the approval necessary for its implementation.

10 ◆ Implement the plan and decide on time frames for progress monitoring and for possible changes to the process.

The process: Implementing the improvement plan.

The process includes a series of meetings and interviews with people or teams working within the organisation or in contact with it (in this case, there must be previous agreement from the organisation, indicating the specific people and/or organisations with whom security can be discussed). The exchange can start with a general introductory meeting, which may be followed by more meetings. These meetings provide the space in which to define diagnostics and discuss the implementation of the improvement plan. Moreover, the meetings can deal with specific items or they can accompany the specific work of the organisation from a security and protection standpoint.

Resistance to the improvement plan.

Now that entry has been gained, a responsible body been appointed and the starting point and process plans been decided on, what resistance might there be from individuals?

As all the processes leading to changes in an organisation, the improvement plan may meet with resistance. However, it will also find approval and support. The point is therefore to see how to harness that support and argue the case against possible resistance.

The most appropriate way to undermine resistance is to genuinely listen to it and try to understand its underlying reasoning. Here again participation, active listening of all view points and expectations are fundamental to a good process.

It is essential that the improvement plan provides for ways to tackle possible resistance so as to avoid later improvisation and run the risk of the plan failing simply because of the earlier denial of possible resistance.

In this chart are some common resistance stereotypes, the reasoning behind those stereotypes and possible responses to overcome those resistance forces.

Common resistance stereotypes	Reasoning behind the stereotypes	Responses to overcome resistance
"We're not being threatened" or "our work is not as ex-posed or contentious as other organisations' work".	• The risk stays the same, it doesn't change or depend on the fact that the work context might deteriorate or that the scenario might change.	• Risk depends on the political context, and the political context is dynamic: so is the risk.
"The risk is inherent in our work as defenders" and "we are already aware of what we are exposed to".	• The defenders accept the risk and it does not affect them in their work. Or, the risk cannot be reduced, the risk is there and that's all there is to it.	• Meeting with inherent risk does not mean accepting the risk. • The risk has at least a psychological impact on our work: it induces at the very least stress which affects the work. • Risk is made of objective elements: threats, vulnerabilities and capacities: vulnerabilities and capacities belong to the defenders and are the variables on which defenders can work. By reducing vulnerabilities and increasing capacities, the risk can be reduced. It might not be eliminated altogether which does not mean that it cannot be reduced as much as possible.
"We already know how to handle the risk", or "we know how to look after ourselves" and "we have a lot of experience"	• The current security management cannot be improved and it is therefore not worth doing it. • The fact that we have not suffered harm in the past guarantees that we won't in the future.	• Security management is based on objective elements that can be worked on. • Look around and see how many defenders have suffered harm although they were highly experienced.
"Yes, the issue is interesting, but there are also other priorities."	• There are more important issues than security of defenders.	• Life is the priority. If we lose it, we will not be able to deal with all the other priorities.
"And how are we going to pay for it?"	• Security is expensive and they cannot be included in fundraising proposals.	• How much do you think security costs? Quite a few security factors are behavioural and do not cost a penny. • Investors will prefer to invest in an organisation covering security issues instead of running the risk of losing their investment.
"If we pay so much attention to security we won't be able to do what is really important which is working with people and we owe it to them."	• The fact that we are affected by security problems does not affect the people we work with. The quality of our work for people does not depend on whether we feel more secure.	• Security is a matter of life or death. • Because we owe it to people, we cannot run the risk of losing our lives. • People run risks by entrusting us with their cases and if we do not work on our security it will affect them too; they might choose to use another organisation that has adequately planned its security and is thus also giving more security to other people.
"We don't have time as we are already overloaded."	• It is impossible to find time in the work schedule.	• How much time do you think security takes? • How much time do we spend reacting to emergencies instead of prevention? (most probably far more than the time required to plan security into our work)

"The community is behind us: who would ever dare hurt us?"	• We are part of the community. The community is not fragmented, does not change both in members and opinions. • The community cannot be influenced.	• The community is not homogenous and is also made up of those who might be affected by our work.
"In our village, authorities have shown understanding and collaboration. "	• Local authorities are not affected by our HR work and will not change their minds. • There is no hierarchy between national and local authorities.	• Organisational historical memory will have examples of local authorities opposing HR work when their tolerance limits have been exceeded. • Local authorities have to implement orders from above. Authorities are made of people who might have an interest in protecting aggressors. • Political contexts change.

Now that entry has been gained, the responsible body has been appointed and has defined both the starting point and the process plans, and that individual resistance has been dismantled, what organisational factors might hinder or facilitate the change?

Organisational factors that can either hinder or facilitate the organisational changes towards a better security policy.

Within the organisation	Factors hindering change	Factors facilitating change
Organisational culture	• Superficiality. Improvisation. Individual oriented. • Security not mainstreamed. • ...	• Team work, awareness of work impact, active listening, consultation, consensual decision making procedures. • Security mainstreamed. • ...
Management attitude	• Authoritarian and dictatorial. Results driven. Distant. Importance given only to leaders and therefore, inclined to designing and respecting rules fitting their needs only. • Non reciprocal expectation that other members are there to serve the management. • Granting themselves privileges. • ...	• In touch with all members. • Recognition of the importance of the contribution of all to the achievement of the organisation's mandate. • Attention given to concerns of all staff and rank and file. • Openness. • Respect of rules. • ...
Organisational structure	• Rigid. • Compartmentalised. • Inappropriate to the work. • ...	• Suitable flexibility. • Coordination and communication fluidity between levels. • Reflecting the needs both of the people and the work. • ...
Knowledge of the security issues	• Centralisation. Partiality. Low awareness of security issues in the field. Lack of objectivity little factual or substantiated knowledge of issues. • ...	• Sharing experience and knowledge. Inclusive. Factual. • Systematic compilation of information and regular updates. • ...

Lack of stability in the organisation; change fatigue.	• Staff turnover. • Absence of historical memory. • Strain due to continuous changes. Absence of work continuity. • ...	• Clear job description and contract with organisation stating commitment to give adequate notice of departure and to hand over knowledge and skills before leaving. • Regular evaluations. • Distribution of tasks that fit the time the staff have committed themselves to stay for. Induction and training • ...
Work overload	• Insufficient and/or inadequate human resources. Stress. Loss of focus • ...	• Prioritisation and (re)distribution of work. • Space to unwind • ...
Work planning	• Security is not clearly prioritised. • Security is not considered in the work plan. • Work plan is spontaneous and does not fit the aim and objectives • ...	• Adequate security planning in work. Security is mainstreamed in the work plan. Adequate consideration is given to activities for which security is seen as insufficient and subsequent decisions are taken as to whether to carry them out if security conditions are not met, • ...

Factors that do not specifically influence the organisational change towards improving the security policy:

- Size of the organisation
- The fact that the people responsible for security do or do not have higher education
- Religion
- Gender
- ...

Standards or good practices in managing protection and security.

Now that entry has been gained, the responsible body has been appointed and has both found the starting point and planned the process, and that individual resistance has been dismantled, that the organisational factors hindering and facilitating the changes have been considered, what are the security and protection best management practices ?

There are several options for managing security within an organisation, and it may be difficult to make a decision about which is the best choice. In the next chart we discuss three models and their pros and cons, along with some solutions.

Structural models	Where are security decisions made	Advantages	Disadvantages	Possible solutions
Centralised model	• At management level, within a dedicated body.	• Easier to check that adequate experience and knowldge exist within the organisation. • ...	• Work overload may inhibit the ability to take proper decisions • May be disconnected from the work in some areas. • ...	• One person at management level with executive ability acts on behalf of the management. • A security is appointed at management level but without executive ability. • ...

Structural models	Where are security decisions made	Advantages	Disadvantages	Possible solutions
Intermediate model	• Important and global decisions: at management level. Specific decisions: made by the people responsible for them in each area involved.	• Management is not overloaded. • Combination of skills and appropriate level. Closer to the actual work of each area. • ...	• Conflicts about security might arise between the management level and the different areas. • ...	• Each person responsible for a specific area takes responsibility for security in that area.A security consultant may be appointed for the whole organisation: a person linked to a given area, for example administration or logistics, takes the responsibility for security and interacts with the person responsible for each different area but his/her own. • ...
Decentralised model	• Security decisions are made at all level because each person has an explicit responsibility for it.	• Better fulfilment, contribution to the organisation's culture concerned with security. • ...	• Discussions might take longer. Might apply mainly to small organisations. • ...	• There might or might not be people dedicated solely to security. • Each person might have that very responsibility in his/her job description or in their previous work. • ...

Standard structural models for security management.

Now that entry has been gained, the responsible body has been appointed and has both found the starting point and planned the process, and that individual resistance has been dismantled, that organisational factors hindering and facilitating the change have been considered, that security and protection standards or best practices have been determined, what about training the staff?

Organisation staff/members' training.

The training may be held with the internal organisational resources (there may be people trained to give security training). The training may also be held jointly with other organisations (sending people to joint training sessions together with people from other organisations). If so, building one's capacities with other organisations might facilitate the subsequent exchange of security information and even the setting up of networks aimed at improving protection. Trust between organisations attending the security training is a must. Moreover, it is useful that organisations share interests and have similar areas of work and environments:, rural and urban organisations for example have very different security needs.

Training can be implemented in many different ways. Arguably the most common are:

- Workshops (preferably in small groups of 10-15 people)
- Individual training (useful for complex tasks or for specific responsibilities, with on-the-job training)
- Conversational mode or semi-formal meetings (couching, active advice).

Carrying out at least some of the training outside the work environment is recommended in order to facilitate concentration and avoid the daily work tension. However it is often counterproductive to hold these activities after working hours (i.e. at weekends) as it might send the wrong message: that security means more work -especially overtime, and that security is not important enough to be included in the normal work schedule.

How to improve the respect of the security rules

Now that entry has been gained, the responsible body has been appointed and has both found the starting point and planned the process, and that individual resistance has been dismantled, that organisational factors hindering and facilitating the change have been considered, that security and protection standards or best practices have been determined, and the staff is trained, how can respect for security rules be improved?

The necessary conditions for the respect of security and rules plans are achieved through the following steps:

- Existence and development of an organisational security culture .
- Ownership of rules and of security plans.
  Participation in their design and improvement process.
  Training to clarify and understand them.
  Persuasion of both their adequacy and effectiveness.
- Drawing up an agreement between the individual and the organisation regarding compliance of security rules and plans.
- Regular intervention by the people responsible for security or information and training purposes, reminding the people of their reciprocal agreements and collecting the opinions of people about the adequacy and effectiveness of the rules.

What can be done in cases of non-compliance by security rules and plans?

I ● Find and solve the causes of the non-compliance (see chapter 2.2).

II ● If the cause of non-compliance is intentional and depends merely on the will of one individual, the following steps may be taken:

a • Talk to the person (as the culmination of a previous process aimed at solving the causes of the non-compliance) in order to generate motivation and commitment.

b • Take the issue up with the relevant work team, in the presence of the individual concerned (this step may sometimes not be adequate, depending on the situation)

c • Apply a warning system (between 2 and 3 warnings)

d • Apply a system of gradual sanctions which can culminate in firing the individual.

It is important to include in the agreement a clause referring to the compliance by the security rules and plans, so that all defenders are fully aware of the importance assigned to security by the organisation.

Summary

Having a security plan does not mean it is implemented and respected. An appropriate process must be devised to manage security implementation, compliance and improvement. The more inclusive the process is, the more information about security needs can be gathered and the more ownership can be achieved.

There is no right or wrong organisational structure: each has advantages and disadvantages. It is therefore useful to analyse them in order to draw up a suitable process and give it as many opportunities as possible to succeed.

The improvement plan has to be **realistic** and **appropriate** to the profile and needs of the organisation

Here are the successive steps of the process towards a better security policy:

- entry must be gained for security
- a responsible body must be appointed.
- the responsible body needs to find the starting point and plan the process
- individual resistance needs to be dismantled by active listening to determine the reasoning on which the individual bases their resistance, in order to phrase a suitable counter-argument (it is not enough to just give an opposite view to the resistance stereotype as the determining factor is the reasoning behind the stereotype: if the resistant individual's reasoning is right, so is their resistance)
- organisational factors hindering and facilitating the change need to considered,
- security and protection standards or best practices need to be determined
- staff / members need to be trained
- security compliance rules need to be improved.

PART III

PROTOCOLS AND EMERGENCY PLANS

In third part of this Manual we are putting forward some sample protocols and emergency plans for use in specific situations.

They are based on good practices shared and learnt in the workshops we run.

They are however neither complete nor a guarantee of good results, as the manual cannot reproduce all the variables of a given context.

This is very much a work in progress, on which we welcome your feedback, as well as new suggestions for protocols and plans.

We will publish updates and developments on the website **www.protectionline.org**, so that defenders can be benefit from them as soon as possible, and we will include all developments in our next edition of the manual.

CONTENTS OF THIRD PART:

Chapter 3.1

How to reduce the risks connected to an office search and/or a break in

A search may best be described as the forced entry into a house, office, or a private space. A search is legal when it is the State that decides about it and carries it out according to laws in force. A search is illegal when the forced entry is against the law (for example a robbery during the night, a search by security forces without the necessary search warrant or a forced search by an armed actor.)

Although the case that follows is the result of a legal search, defenders will also be able to extract rules applicable to illegal searches and complete them with information contained in the chapter on security of houses and offices.

The State may lawfully carry out a search. The law in force will need to be in line with the international standards on human rights and the protection of democratic freedoms. However, it can be a serious problem if, against international standard, searches are used as a standard method to continually harass and pursue in justice human rights defenders and social movements through routine searches.

No defender can claim that a search is an "unexpected" event (as with any other risks), all the more that a search can be absolutely legal. No risk can be reduced to zero. We then need to reduce as much as possible the related threats/ consequences of the search risk.

How do we achieve this? By using the risk equation and listing all threats/consequences (consequences may be assimilated to threats). Then, for each threat/consequence, list the related vulnerabilities and capacities, and start working on them...

Threats/consequences linked to searches.

A search generates threats/consequences:

a • The threat that during a search somebody may suffer physical or psychological harm.

b • The threat that information may be taken away, lost or destroyed.

c • Related to that, that information may then be used inappropriately by a third party.

d • The threat that contentious objects may be "hidden" (arms, drugs, documents) in order later to proceed "legally" against the organisation.

e • The threat/consequence of money and specific properties (such as computers,...) being stolen or destroyed.

f • ...

a ◆ The threat that during a search somebody may suffer physical or psychological harm.

No one can predict how a search will be carried out and what its impact will be. However, having as much advance information as possible about a search can contribute to avoiding behaviour and stress that could add to the likelihood of physical and psychological harm. It can contribute to raising awareness of risk triggers and to maintaining positive behaviour.

Vulnerabilities:

- not knowing what a search is about
- believing that opposing it will help the situation
- no medical insurance
- ...

Capacities:

- knowing how a legal search may be carried out
- knowing what department may issue search warrants and being in possession of the name of the current reponsible officer (before and during a legal search)
- knowing what a search warrant looks like
- knowing what the legal rights of the searched organisation/individual are (including the right to ask to see the search warrant and possibly to request legal assistance)
- having access to legal assistance (during and after the search)
- how not to put up undue resistance
- if a search is carried out with violence, it is important that the people stay in a group to reduce the risk of being mistreated individually
- …

The organisation consider posting in a visible place:

- a sample search warrant

- all corresponding legislation (rights and duties of both parties)

- a list with the names and telephone of the organisation's lawyer, doctor, psychologist, the closest hospital…(This list should also be visible in other parts of the office so as to increase the possibility of quick access to it by staff members present)

This information is legal and public. It can therefore be visually accessible by both parties. This may not prevent a search (either with or without a search warrant). It might however help to reduce stress among those being searched. It might also contribute to notifying the searcher that the searched individual or organisation is aware of their rights and that they will take action later in case the search goes beyond legal prescript (deterrence).

b ◆ The threat that information may be taken away, lost or destroyed.

In general, most organisations keep more information than is needed. Of this, a high amount is hardly ever used and is not confidential. In other words, only a small amount is confidential and this should not be accessible to searchers. Absolutely confidential information usually includes: lists of people (project beneficiaries, witnesses in cases); crucial evidence in legal cases; specific cases and analysis.

Information deemed public or not contentious can be kept in the office for the searchers to take (such as one does when travelling with money, keeping visible only the amount we can afford to lose to robbers).

A proper information security policy means that many of the consequences connected to the loss, theft or destruction of information are considerably reduced.

It also means that the defender should not feel the need to expose themselves to protect information (in any case, life must come first) ; this will decrease the likely stress generated by the search, thus reducing the risk of violence and injuries both physical and psychological (taking care of the above threat/consequences).

Vulnerabilities:

- information not stored/filed according to agreed distinction between confidential or not.
- sensitive information held on paper
- electronic information not encrypted (files and attachments).
- inadequate office and house security: not enough barriers and filters to prevent access by undesirables or at least allow time to shut down a computer or hide a document.
- …

Capacities:

- regular backup copies (at least weekly) of information stored on computers, and kept in a safe place. In case of a search you will therefore largely know how much information is actually exposed (depending on the date of the search vs. date of the last back up / storage of information)

- copies or photocopies, or even better, scanned copies, for keeping records of essential documents in a safe place. If necessary they can be distributed around other safe places).

- adequate office and house security measures.

- warning at the beginning of a search in order to obtain legal support (lawyers) and requests from other organisations to provide assistance and witness the search, at least from outside. This will put pressure on the perpetrators in the hope that they will comply with the law during searches.

- ...

COMPARISON OF DIFFERENT COMPUTER BACKUP SYSTEMS

Storage medium	Advantages	Disadvantages
CDs/DVDs burning	Many computers have CD/DVDs burners. Easy and safer transportation and storage of the backup DVDs/CDs.	In case of a high amount of information, many CDs are needed, which makes the whole process longer and more complex. Anyone managing to obtain the CDs will have access to all the data.
Flash disk	Same as above.	As above though easier to store and therefore, less likely to fall on unwanted hands.
External hardware	Holds a lot of information and it doesn't take much time to copy over. Can be equipped with access codes in order to protect the information.	Cost (200-300 US $).
Server at a remote location	Can hold all the information, is quick, cannot get lost or stolen.	You need a broad band internet connection and encryption Server companies might be 'forced' to give the archive to the searchers ('state security claim').

c ◆ The threat/consequence of the information being taken away and used by the third party.

High likelihood of consequences for the organisation and for the people mentioned by the information.

Consequences for the searched organisation

Vulnerabilities:

- no advance consideration given to possible reaction procedures
- neglecting ethics, bad accounting, pirated software (might mean legal proceedings against the organisation)
- ...

Capacities:

- Back up copies
- Reaction plan in place
- ...

Consequences for the people mentioned on the information.

Vulnerabilities:

- not having previously discussed the possibility with the people involved
- not having fast access to them
- ...

Capacities:

- to have explained the existence of the risk and made as sure as possible that it will not happen out of the negligence of organisation/people.
- to have planned together the emergency reaction (resorting rapidly to the plan, , protection measures, hiding places, etc)
- ...

d ◆ The threat that contentious objects may be "hidden" (arms, drugs, documents) in order later to proceed "legally" against the organisation

Vulnerabilities:

- office space is full of objects and papers not related to work (personal objects, scattered magazines... (it is more difficult to spot if something is being hidden intentionally during the search, or if a previous visitor has hidden/left a contentious object/document which might then be "casually" found by the searchers

- no inventory of office material at all, let alone a recommended registered inventory with a lawyer
- only one organisation person present during the search
- ...

Capacities:

- where possible, (in the case of a legal search)[1] , people are prepared to arrange themselves in the various corners/rooms of the office (for example each person on his/her working place) so as to be able to observe what happens during the search. it is also easier this way to notice if anything is being taken illegally.
- after the search (no matter what type of search), the organisation carries out a complete check of the office or place (if possible with the assistance of external observers), recording (even photos) all that can be found and making sure that what does not belong to the office/was not there before the search, is clearly reported and not touched (be aware of finger prints). Make a record also of missing items.
- File a report with the police and follow legal provisions in force.
- ...

e ◆ The threat/consequence of money and specific properties (like computers,...) being stolen or destroyed.

An illegal search will most probably will entail the theft of items.

Vulnerabilities:

- high amount of money and valuables kept in the office
- unprotected items
- no inventory of office material at all, let alone the recommended registered inventory with a lawyer
- no insurance against theft
- ...

Capacities:

- arrange office staff in various places in the office in order to observe the search[2]

[1] If a search is carried out with violence, it is important that the people stay in a group to reduce the risk of being mistreated individually

[2] Again, if a search is carried out with violence, it is important that the people stay in a group to reduce the risk of being mistreated individually

- warning at the start of a search in order to obtain legal support (lawyers) and so that other organisations may be requested to provide assistance and observe the search, at least from outside. This will put pressure on the perpetrators in the hope that they will comply with the law during searches

- ...

How to confront and reduce the threat of the search itself.

If a search follows the standard international legislation and has a legal and legitimate goal then there is no point in even thinking about confronting or reducing the threat of a search. You have to open the door and consider only the previous steps on acting on the consequences. However, if searches are used as a systematic way to hinder the work of HRD and social organisations, then corresponding action should be taken.

In order to confront and reduce the threat of a legal search, the best strategy is to raise their political cost through public campaigns and advocacy, preferably in collaboration with other organisations and institutions.

If there is a risk of an illegal search (or robbery) it is important to improve as much as possible the security of the house, office or the premises.

This all applies whether your office/home is in an urban or a rural area.

Summary

How to reduce the risk of a search.

Searches can be both legal and illegal (when illegal it is akin to breaking in).

And just as for any other specific risk, increase the political cost of searches

Use the equation and unfold each element as far as you can go.

List the threats/consequences and their respective vulnerabilities and capacities and work on them:

a • The threat that during a search somebody may suffer physical or psychological harm.

b • The threat that information may be taken away, lost or destroyed.

c • Related to that, that information may then be used inadequately by the third party.

d • The threat that contentious objects may be "hidden" (arms, drugs, documents) in order later to proceed "legally" against the organisation

e • The threat/consequence of money and specific properties (such as computers,...) being stolen or destroyed.

f • ...

CHAPTER 3.2

Secure management of information

Human Rights defence organisations manage information that in an environment hostile towards defenders could be used to affect the safety of the organisation, other people and institutions. It is therefore crucial to set up a secure information management procedure and a reaction plan to any incident affecting the security of information managed by the organisation.

Secure management of information: prevention procedure

Data held by HR organisations may in general terms be grouped into two categories according to its level of sensitivity: high confidentiality, and low confidentiality.

Any piece of information managed by us undergoes four separate steps before reaching us and before leaving is (where relevant). We will outline the security needed at every step along its way.

1 • Source- information collection, at meeting point.

2 • Transfer of the information,

3 • Processing and storage.

4 • Distribution.

1 • Source- information collection at meeting point.

The main problem here is protection of the information and the people affected by it.

The person living the information requires a route between their home / office and the meeting point; a meeting point (the place where the person giving the information meets up with a member of the organisation); this meeting point may be that person's home or place of work, the organisa-

tion's offices or any other place; and a route to leave the organisation's headquarters (trips to and from the meeting points).

A secure place and conditions for meeting are required, as well as a route for the information to arrive and leave the source, and a route for the arrival and exit of members of the organisation who will in turn transfer the information.

Information management security begins even *before* receiving it.

- Does the organisation even need to obtain this information?

  Will the organisation be able to use the data to improve its work or better meet its aims and objectives? If not, it is better that the organisation **does not receive** the information; if it falls outside its sphere of competence, our organisation may refer the person to another organisation, without taking on either the information or the case.

- Communicate to the person giving the information who we are, what our objectives and work are, how the information will be manager by the organisation; the sort of information we require, how we will look after it and use it- and what they can expect from us. It is fundamental and ethical that the person giving the information should know in advance (either directly or via third parties) the risks of passing on the information, and the uses to which the organisation might put it.

It is not enough to suppose that the person concerned is aware of all this. It is important for us to explain it to them so that we are sure that he/she knows it. It is also important to define with them possible security measures.

The meeting place must be as secure and anonymous as possible. In all likelihood the person's home will not be a secure place, as the arrival of an organisation staff member would be easily noticed. The organisation offices may offer more security (as long as confidentiality is respected), or another fairly public place in which people are coming and going routinely (e.g. parish building, community centre) as long as confidentiality is once again respected. If the meeting is arranged in inappropriate place, it may be adjourned to a more secure location according to the sensitivity of the information being transmitted.

One might also consider resorting to an official cover story: the person leaves home with an official pretext. They will need to build the pretext: dentist visit (show tooth ache), medical visit (any illness), market, etc the person will need to come back home with real proves (medical prescription and drugs, shopping that they would not have found in their home place)

Do not forget that security problems may arise for the person giving the information after the meeting at the agreed meeting place.

2 ● Transmission of information

Information may be gathered in various mediums: memory, printer, notes written by hand or on the computer, photos, etc...

The most secure routine method of transferring information is by laptop computer, memory stick or CD Rom equipped with security encryption. The meeting can be recorded, photos can be stored and notes can be taken. All other mediums are deemed to be less secure, which increases the risk of the transmission process.

Confidential information should be carried only by organisation members who are aware of what they are carrying.

Too often human rights defenders travel with their whole note books containing important information not necessarily related to the specific mission. They keep the notebook until it is full instead of travelling with only the amount of paper or material they need. The same goes for the content of USB flash disks, computers and other information support.

3 ● Storage and processing of the information

Once the information has reached the offices of the organisation it is usually more secure (according to the weaknesses of the office- see chapter on security of houses and offices).

Standards of particular relevance to information are:

Paper archiving of printed documents: this should be used only where necessary; necessary documentation on particular cases should be handed over in person. Paper information should be stored in lockable metal boxes; the use of a strong room should be considered for storing these.

One may also consider the possibility of distributing the papers between several safe places or send them to other places with the same care as illustrated in "transmission of information". Information can also be scanned, encrypted and sent to a trusted body (for example, to an international counterpart).

Encryption systems and codes should be used appropriately.

Make weekly back-up copies, and store these copies, also encrypted, securely, in a safe or other place.

4 ● Distribution of the information

General criteria regarding the distribution of information include the following points:

- Cross check the information

- Where the organisation is the only source of information on certain facts, there will be increased risk and contingency plans will be needed.

- Informed consent should be obtained from the persons giving the information, particularly where these persons are identifiable locally as the only source of the information.

- Any written information leaving the organisation or allied organisations should be considered "public" due to the risk of it falling into the wrong hands, or the day to day vagaries of means of communication.

- It is crucial for the organisation publishing the information to have a dedicated publication policy; this should include the main security standards applicable to the publishing of the information (among which rules to word the information itself).

Access to information by persons who are not members of the organisation (helpers, volunteers, etc...)

For the safety of the organisation, third parties, helpers and volunteers, access to these digital and physical archives must be restricted (decide according to the type of case) and must come under the particular responsibility of a staff member of the organisation.

t may be useful to incorporate into the contract or work agreement documents of helpers and volunteers a confidentiality clause that should be abided by at all times. This confidentiality clause should also be included in contracts of personnel subcontracted by the organisation.

Secure data management: reaction procedure in cases of theft or loss of the data.

Theft or loss (it may be hard to determine which it is) of data held by the organisation should cause us to react as though the information will necessarily fall into the wrong hands, and that malicious use will be made of it, that may affect third parties (whether those reporting the information or colleagues, etc...) or the organisation itself.

If, despite all the prevention procedures, a loss or theft of information occurs, it should be treated as a serious security breach, and the following steps should be taken:

1 ◆ Immediately inform people at the organisation.

2 ◆ Assess the quantity and sensitivity of the information lost or stolen, according to whether:

it puts at risk the people directly affected by the information, third parties or the organisation, and why (or the vectors for risk). This assessment should be carried out for every type of information stolen, where several types were stolen (e.g. lists of people, references and information collected on individual cases).

3 ◆ Assess the subsequent informing of people and institutions potentially affected so that they may take appropriate steps to protect themselves (should always be done discreetly).

4 ◆ Assess informing the authorities and reporting the events.

5 ◆ Where necessary, set in motion any other steps needed to avoid damage in case the lost or stolen information might used. .

The organisation will also need to decide how far its members can expose themselves to risk in order to protect information: for example in case of a violent search, one ought to consider if it is "worth" resisting.

Summary

Secure information management requires prevention and reaction protocols.

Prevention ought to consider 4 moments:

1 • Source- information collection, at meeting point.

2 • Transfer of the information,

3 • Processing and storage.

4 • Distribution.

Reaction ought to at least include:

1 • Informing the responsable persons in the organisation

2 • Assessing the quantity and sensitivity of the information lost or stolen

3 • Assessing the subsequent informing of people and institutions potentially affected

4 • Assessing informing the authorities and reporting the events.

5 • Steps needed to avoid damage in case the lost or stolen information is being used.

Detention, arrest, abduction and kidnapping of a defender

"No news from a defender"

When we have no news of the whereabouts of a defender, the first challenge is to find out exactly what has happened to him/her, and it might take some time. Several things may have happened:

- The defender may not **want to**, **or may have forgotten to** get in contact with the organisation: he/she may have decided to go away for the weekend or on a visit without telling anyone (or may want to "disconnect"). He/she may have found themselves without a telephone or any other means of communication, or may not be bothered about checking in. They may not have wanted anyone to know what they are doing (sometimes successfully). They may (and this is the least frequent option) have forgotten or not realised the fact that their whereabouts might concern their colleagues.

- The defender may not have been able to get in contact with the organisation for **technical reasons**: this can happen when the defender is, unpredictably or unexpectedly, cut off from means of communication in a place that is too remote. This might happen during a trip when the defender happens unexpectedly to be in a place with no communication, when the road is blocked, or he/she has to take an alternative route, or where he/she has to make an improvised change of plan during, leading him/her to a place without communication. It may also be that the expected means of communication is damaged in some way (broken cell phone, no credit, dead battery, collapse of the local telephone network, etc.).

- The defender might be unable to check in due to **illness or hospitalisation** (e.g. due to a traffic accident, previously unsuspected illness, or a worsening of an existing illness)

- The defender may have been **detained**, **arrested**, **abducted** or **kidnapped**. All have in common the characteristic that the defender is deprived of his/her freedom of movement and could experience anything from polite pressure to a life threat[1]. In some

[1] In this chapter we will draw on some of the contents of the useful security manual by van Brabant (2000) (chapter 13)

cases the defender may be able to check in with the organisation, meaning that the organisation will have more information about the si-tuation.

Detention means that organisation members are kept under the control of a group (of soldiers or militia, a local authority, etc). *Arrest* is the term used to describe detention by security forces (so that in principle law can be invoked). *Abduction* refers to the forced capture and removal of a defender in an illegal way for political reasons. *Kidnapping* refers to forced capture and detention with the explicit purpose of obtaining concessions from the captive or others. In this chapter we will use preferably the term *detention* for the sake of simplicity.

In general we should say that in most cases not having news of the whereabouts of a defender usually falls into the first two categories (not wanting to/ forgetting to communicate, or not being able to for technical reasons). Let's see how to prevent and react in these cases.

Prevention tips for avoiding a "No News" situation regarding the whereabouts of a defender

The defender does not want to, or has forgotten to get in contact with the organisation.

- Every member of the organisation and particularly those most at risk must be aware of the fact that others will be concerned if they do not give news of their whereabouts. If they wish to be out contact, they should notify colleagues of this, including details of when they will be back in regular contact. In the case of defenders at high risk, it may be inadvisable for them not to be in regular contact.
- It is important to establish checking in routines for staying in regular contact with the organisation (usually with one or two named people) This becomes essential as levels of risk rise for a defender (because they are travelling to a risky area, or have received threats, etc...)

The defender is not able for technical reasons to make contact with the organisation.

- Pre-agreed checking in times should be established, and communication problems should be anticipated for those times: for example, if a check-in time coincides with a trip, thought should be given as to how and when it may be possible to communicate (by cell or landline telephone, or other means) in order to be certain that it will be possible, and to ensure that damage, breakdowns, expiry of credit or battery failure will not prevent communication.
- Plan alternative means of communication (via third parties for example).

The defender is no able to communicate because he/she is ill or in hospital.

- Lists should be kept of telephone numbers and addresses of all hospitals and health centres in the visited area, and where possible details of how

to get updates in traffic accidents (bus companies, highways police, contacts along the route, etc...).

- Defenders should not undertake trips unless they are in good health.
- Use the safest possible means of travel (including buses or other means).
- Defenders should have up to date health and accident insurance.

Preventing detentions.

It is not easy to anticipate preventing detention. The crucial aim is to reduce the reasons and the exposure that might cause or facilitate the detention of any member of the organisation.

- Ethical behaviour of individuals and organisation is crucial so as to reasonably exclude personal and organisational breaches of common law, Breaches of common law may of course be used as a pretext, but the organisation's lawyer will know what to do. Furthermore, the detained defender will know that steps are being taken and can recite them to themselves almost to the actual timeline and "remain calm" (psychological impact), knowing that outside action has started. There is no need to challenge the authorities or to provide an opportunity for them and expose oneself to more risk than what s/he is already undergoing.
- In cases where breaches of a law are used as a political action, a full risk assessment becomes necessary and a damage limitation strategy must be prepared, given the increased risk incurred by defenders.
- Legal detention can of course be a pretext. It might or not be upon a summons and/or a warrant and can happen any time, at the office/house or during a trip. The point would be to prevent an arrest when the defender is alone so as to reduce the consequences related to the detention itself. What is ultimately needed is a political action strategy aimed at deterring the authorities from arresting defenders; nonetheless, the tendency in many countries seems to be to judiciarize defenders and imprison them for various reasons, including ones unconnected to their work.
- It is no easy to prevent abduction. Apart from carrying out a costly risk assessment when a threat of abduction is suspected, it is crucial to reduce exposure in areas where the threat may be carried out, ensure one is never alone, and weigh up any action that may facilitate an abduction.
- Abduction can be carried out by common criminals (whether as a pretext or not) or by legal actors and/or para-legal actors, and/or armed political groups etc. It can potentially happen anywhere, but most probably will happen when the opportunity is either created by potential aggressors, or handed to them by the defender and preferably with no witnesses around. Therefore, abduction is less probable at the office during working hours, at the house during daylight hours, etc.(see example of death threats against an organisation leader in chap. 1.7)

The difference between illegal procedures of a legal detention and aggression/abduction is so thin that we recommend that human rights defenders consider all items of both parts not as mutually exclusive rather as

mutually complementary. However, we consider it important to state the difference between the actual meaning of both detention and abduction for psychological and practical questions.

- The aggression/abduction prevention procedure should take into account the defender's day to day work in the usual area of defender's activities, free time etc., and definitely during field missions, whether planned by the organisation and/or by invitation. Be vigilant and double-check all invitations from unknown parties.

WE SUSPECT THAT A DEFENDER HAS BEEN DETAINED (OR ARRESTED, ABDUCTED OR KIDNAPPED)….

When can we suspect that a defender has been taken against his/her will? Well, if we do not have direct news from the defender, we must suspect it when we reasonably disregard the first three options… Realistically, the procedure for reaction to a detention or a suspected detention follows the reaction procedure used when a person fails to report when s/he is supposed to.

So, when we have no news from a defender we must start searching, in order to disregard any of the three first options. It is difficult to be certain that we have excluded any of the first three options. For this reason it is important to set a time limit before considering the fourth option: 3 hours with no news, 6 hours, 12 hours…. Depending on the context, circumstances, level of risk, awareness of the defender of the need to report, etc. The shorter the time, the more risk of making mistakes if we issue an alert; the longer the time, the bigger the delay in taking necessary action. Not an easy decision to make!

Warning: a report may fail to be filed through an oversight, through the negligence of the person who should have done so, or through a lack of means of communication- these should all be anticipated when planning the reporting schedule for the mission.

Remember: We may react to a suspected detention or a confirmed one.

It is crucial that the reaction of those detained and of the organisation involved be harmonised, and attempt to achieve the same objectives. It is for this reason that all the members of the organisation should be well acquainted with reaction procedures.

DETENTION (arrest, abduction, kidnapping):

A detention (arrest, abduction, kidnapping) may vary in length from a few hours to even years. Resolution will most often be achieved by setting the person free, or it may turn into kidnapping situation when a objective is sought beyond the mere detention, or in some serious cases –abduction- it may lead to injuries or death, or "disappearance".

Detention should be dealt with from three points of view:

- from the point of view of the detainee(s)
- from the point of view of the organisation upon which the detained persons depend,

- from the point of view of the family and relatives of the detainee(s)

General objectives when dealing with detention:

- reduce the likelihood of a detention occurring.
- be informed as quickly as possible of the chances of a detention.
- outline how to react in such a situation:
  - Immediate reaction
  - Medium-term reaction

In order to keep this manual as simple as possible we will cover detention (including arrests) and kidnapping separately.

Detention of a defender: immediate reaction

Objectives and steps of immediate reaction to a detention:

Establish an ad hoc working group to react to a detention.

1 ◆ Protect the life and freedom of members of the organisation.

2 ◆ Locate geographically the detained persons, using a map, the trip plan, the last contacts made, call contacts and actors in the field, etc...

3 ◆ Work out which armed actor has detained the person, why, and to what end.

- Using the geographical location of the detained person(s), along with background knowledge (you may have to infer causes for the detention if you do not yet know them). It will thus be possible to arrive at a reasonable guess of who is detaining the person, or at least arrive at a short-list of possible suspects.
- Contact authorities (if adequate and necessary and possible)

4 ◆ Achieve the release of the defender from detention unharmed.

□ As a general rule, it is important not to focus on getting an agreement rather on getting an actual "exit" or release, leaving negotiations until after the defender has been.

□ Assess the armed body concerned (in collaboration with regional authorities where possible/necessary), either directly in the case of a security forces body, or by using intermediaries- the assistance of other bodies such as churches, local dignitaries or elders, the International Red Cross committee, etc... For this reason it is crucial to be able to rely on these contacts. This assessment will aim to ascertain the reason for the detention, and attempt to obtain the immediate release of the defender detained.

□ Consider alerting other human rights defenders and humanitarian organisations so that they are aware, and are able to take the necessary steps jointly for extra weight. Where abduction with probable injury to the defender is suspected (such as an abduction carried out by a "hit squad"), it is important to act as quickly as possible and to focus action as much as pos-

sible on the obvious leaders (where relevant) of the group responsible for the abduction, or on the political bodies close to those responsible that are most likely to react to national and international pressure..

- Alert consulates if the detained person is from another country.

Detention of a defender: medium-term reaction

If a defender is detained, and we do not anticipate being able to secure their release in the short term, medium-term objectives and steps should be introduced without losing focus on short-term objectives.

Objectives and steps of a medium-term reaction to a detention.

1 ◆ Retain focus on short-term reaction objectives.

2 ◆ In the case of an arrest, on top of identifying as quickly as possible who is holding the defender, try and obtain a transfer to legal custody or to a security service over which there is some influence. In this case, try and obtain adequate legal support as quickly as possible (ideally prepared in advance). The risk of ill-treatment and torture may thus be reduced.

3 ◆ If the defender continues to be detained, try and attend to their personal needs -safety, food, healthcare, contact with their family and the organisation, etc. from the beginning of and throughout the process (this must also be planned ahead – see below: measures aimed at the family and relatives).

Reactions by the detained persons

- Remember the steps and plans previously prepared in view of the possibility of such situations. It is important to know what the right sequence of steps is in the event of a detention or an arrest, in order to minimise uncertainty, use one's strength in a controlled way and plan simple resistance objectives.
- Remain calm. Defenders know the organisation has a reaction protocol and that steps are being taken; they can recite them to themselves almost to the actual timeline and stay calm.
- Everything said and done should be aimed at preserving the life and safety of detained persons.
- Make contact with the chief of the armed group, and instigate dialogue with him, using basic institutional arguments with the aim of obtaining the release of the detained persons and their return to where they came from, or to release to any other safe place (do not intend to negotiate a "settlement").
- If this is not permitted, seek permission to use any means available to alert the organisation on your position; do not attempt to call without permission if you under guard, as this may cause more risks than doing nothing.
- If the detention is being carried out by security forces, use the legal arguments provided by the organisation for these cases.

- Stay calm and do not forget that the organisation is rapidly deploying all its security systems as time goes on.

Measures aimed at the family and relatives:

- Inform the family and relatives if the person is not going to be released soon. Establish and maintain trust.
- Develop a clear approach towards the family. Provide support and keep them informed (appoint a link person for the family).
- The family will want time and attention from the organisation. Expect fluctuating attitudes and initiatives from the family.
- In case of long-term arrest or imprisonment, it is important to plan support for the family of a detained defender.

Abduction and kidnapping of a defender[2]

From the point of view of the organisation

Managing a kidnap crisis is a changing process that can last from anywhere between a few hours and months or even years. Key issues are the mobilisation of a competent crisis management team; dealing with the family, the authorities and press; communications and negotiations with the captors.

Communicating and negotiating with the captors

Kidnapping, as understood here, is deliberate and for a purpose. The captors will usually establish contact to make clear their demands and conditions.

The crisis management team should retain control over the negotiations, but avoid making direct contact with captors; the purpose is to create a time lag to allow for internal and external consultation and decision-making. You can if necessary ask for proof of life and for proof of the identity of the captors, and encourage and demand good treatment of captives.

If kidnapping is a real risk, it is important to previously agree on certain rules and procedures in relation to ransom and requests from abductors, where possible in line with similar organisations, and publicise them.. In any case, earlier similar events will inform about the likely stages of a kidnapping.

From the point of view of the abducted/kidnapped defender

- The most dangerous moments, when the captors will be tenser, are during the abduction, when the abductee is moved hastily because the captors fear that the authorities are near, during a siege situation and during release.

- Your captors will want you to be quiet; you may be blindfolded, beaten and even drugged for that purpose. It does not make sense to cry or struggle to oppose these tactics: actually being quiet might help you to avoid them (unless you reasonably expect that, during an abduction, crying or yelling can get other people to help you).

[2] For this subject we will draw extensively from van Brabant (2000)

- The place and conditions in which abductees are held can vary widely. You may be kept in the same place or moved several times; you may be alone or with other captives. It is common for abductees to develop some sort of relationship with their guards and find it difficult to adjust as guards change.

- Obey the orders of your captors without appearing servile; avoid surprising or alarming them.

- Try to maintain physical and mental health.

- If you are in a group you should try not to be separated, as being with at least one other person can be a source of support. It is important however to be prepared for separation and changes, and in general for uncertainties that each day might bring and which will need to be faced.

- Securing release is not your problem but that of your organisation. Never get directly involved in negotiations for your release. This will only complicate matters. If asked to talk on the radio, telephone or on video say only what you are asked or allowed to say and refuse to negotiate even if pushed to by your captors.

PREVENTION PROCEDURES: REDUCING RISKS OF DETENTION OR ABDUCTION DURING A TRIP

Risks of detention or abduction are particularly high during a trip or mission because the defender is more exposed, has less contact with his/her usual surroundings, and those around him/her may delay reacting to a threat or attack. For this reason, we state the risks linked to a field mission include most of the threats /consequences related to the whole work of the defenders.

For example:

check points ⇨ arrest ⇨ detention ⇨ ...
Aggression ⇨ abduction ⇨ violence ⇨ ...
Loss of information ⇨ impact on witness ⇨ impact on organisation ⇨ ...
Transport ⇨ public / private ⇨ ...
Leisure time on the field ⇨ lowering guard ⇨ security incidents ⇨ ...
Communication ⇨ phone ⇨ face to face ⇨ ...

We would like to insist on the risk of detention / abduction during a field mission and recommend that the prevention protocol for field mission include at least:

- preparation for all missions, both in the field or to urban areas such as neighbourhoods, where relevant.
- do not travel alone.
- adequate information on the background of the area and actors to be visited (actor mapping, field force analysis see chap.1.1.)
- defenders should know entrance and exit routes for the places involved.
- every person involved in the mission must hold relevant valid identity documents.

- alert the organisational emergency contacts who are on standby during the whole field mission (from the moment it leaves until the moment it is back)
- prepare the mission in accordance with procedures: include the agenda and work to be carried out, and it should also form part of the organisational security manual.
- plan regular updates on the state of the mission (usually by telephone, at times previously agreed). It implies, if possible, to check whether the route and final destination zones have got telephone reception. If it is not possible to check or there is not reception, one might consider the possibility of resorting to trusted people living on the way to confirm that the team has been seen by.

  It is important to decide how long the designated person should remain on standby waiting for a report call after having tried unsuccessfully to reach the team, before getting worried. Remember that it is easier to reconstruct an abduction within a time frame of a few hours than many hours.
- assess the security of the chosen means of transport (this might at times be the organisation vehicle and at times public transport so as to be surrounded by potential witnesses). In the case of public transport, assess whether to sit together or separately and pretend not to know each other. This might give the possibility for at least one member of the team to alert the organisation. To intervene might mean losing that chance.
- If trips are made in one's own vehicle, it should be in working order at all times (respect speed limit and traffic code). Do not pick up hitchhikers.
- where relevant, distribute appropriate information to the civilian, military and community authorities, as well as to those responsible for the mission (so that they take responsibility for the safety of the mission and do not simply say that they "did not know").
- present a prepared argument that explains the aims and mandate of the organisation, in a way that is as acceptable as possible to armed groups and security forces (it is better not to adapt the argument to the armed group faced, as it may be difficult to identify who they are and it would be easy to make a grave mistake).
- assess the best time to leave for the field (at times, because of hot weather, it may be preferable to leave at dawn regardless of security). In the event of an attack right after leaving for the field however, the organisational emergency contacts might not yet be operational; the first moments after an abduction are crucial in being able to keep track of the person.
- Do not travel after dark.
- Do not at any time obviously display valuable items (such as cameras or video cameras).
- Behave appropriately during the trip.
- Usually, get the organisation to obtain permission for the work from the community visited (and where possible to negotiate at least tolerance from armed groups).

In the case of a field mission following a call from a third party, also:

- Be sure of the identity of the caller (cross-check with trusted organisations)
- Cross check details about events mentioned
  - assess whether it is important to actually go to the field or if it would not be safer for all if the information were to travel to the organisation (see information management: prevention and reaction protocol)
  - assess whether is necessary to go there and then, right after the call, especially if the calling person is unknown (information should at least be cross-checked first). Also, one ought to consider that the field mission is not going to prevent the events as they have already happened, hence the initial call. In general, the best advice is to avoid improvisation and changes in plans whilst visiting a risky area.

Summary

We understand that detaining a person can be a legal procedure. When it goes beyond legality it can be considered as an unjustified deprivation of a person's freedom. Its duration may vary in length from a few hours to years…

Detention should be dealt with from three points of view:

- from the point of view of the detainee(s)
- from the point of view of the organisation upon which the detained persons depend,
- from the point of view of the family and relatives of the detainee(s)

General objectives when dealing with detention:

- reduce the likelihood of a detention occurring.
- be informed as quickly as possible of the chances of a detention.
- outline how to react in such a situation: immediate reaction and medium term reaction.

Abduction is illegal and can happen any time, usually when the opportunity arises. It is one of various possible consequences of "aggression". Therefore, security measures will be similar to those regarding prevention of aggression (Ch. 1.5.): reduce physical exposure as much as possible…

Chapter 3.4

Security and free time

Reflection:

Generally speaking, security rules are followed as long as they do not clash with personal interests. It will, therefore be easier to tackle office security, for example, than free time. Yet, free time is a fundamental element of both individual and organisational security. It requires discussion and understanding of how personal needs can interfere with security.

Free time

Here are a few questions and reflections to help the organisation draft its free time policy. It is important, as with any other security item, to explore them as far as possible even if this exploration might breach privacy (security incidents can breach privacy too…).

We begin with two important reflexions:

- If someone wishes to attack an organisation, they will probably not attack the best protected people or those who follow safety rules, but rather will target those with weak spots, particularly during their free time (at night and weekends, etc...)
- If an organisation has 10 members, of whom one or two do not abide by safety rules during their free time, it is the whole organisation, not just the one or two, who are at risk because the whole organisation would be affected by an attack against those two..

The underlying question is always: "is there a security risk attached to..." If the answer is "no", then it is fine. If it is "yes", then it needs to be explored and decided whether there are ways to satisfy a personal need in a protected environment or decide whether the need needs to be postponed for safer times or simply dropped as incompatible with the security of a human rights defender.

Do we care about security only during working hours or 24/7?

Although it is difficult to make the distinction between the organisation's policies and the autonomy of every member during their free time, the prevention of attacks and reactions to them make no difference between attacks during work-

ing hours and those carried out during free time... We must not forget that if a person decides to attack an organisation via its members, they will not do it in working hours, but at times when defenders are at their most vulnerable. A person planning an attack against a defender will search for an opportunity to do so. We must also bear in mind that an attack at night, or on leaving a club, etc. will be much easier to cover up…

In countries where drinking alcohol is a social custom, is drinking to the point of getting drunk a security risk?

Getting drunk in a public place has a definite impact on security. The de-fender might talk, their behaviour is altered and they might not be aware that they are being deliberately questioned or challenged. There is a definite impact on the organisation image, if not directly on the physical security of the human rights defenders. And remember that a drunk defender provides an opportunity for any hostile group to attempt to take advantage of when contemplating an attack on the defenders' organisation (the same is true for other drugs). The use of alcohol and other drugs with regards to security should not be examined neither from a moral nor a health point of view, but as an objective fact affecting security.

Can hidden relationships and affairs affect security?

- There have been cases of human right defenders not reporting back to their organisations because they had a private affair. The organisation had already alerted its emergency contact only to find out that the defenders were perfectly fine and unaware of the trouble caused. This type of situation obviously gives others an opportunity to discredit the organisation and the defender concerned by drawing attention to the image and ethical implications. Some emergency contacts might even decide to withdraw from the organisation's early warning system.

- The problem is not the affair, but how the affair may affect communication and security. We reiterate that it is not a moral or health issue but a security one. It is important that the organisation is able to deal with these issues in a clear way and that it look for ways to address them.

- What if a defender's friend is viewed as suspicious by others in the organisation? Can the organisation interfere?

- In what ways can information be passed on to friends, families and relatives? Is the human right defender responsible for how that information might be used?

How defenders use free time therefore has a potential security impact. The point is not to deny the need to enjoy free time but rather see how it can be enjoyed.

All defenders' organisations at risk need a policy for the enjoyment of free time, from evenings to holidays. Special mention is necessary for the public use of alcohol and other drugs, how hidden relationships may interfere with security and how free time may affect the image and security of the organisation?

How do we treat the confidentiality of information?

And because information can leak out any time, even during free time, here is an extra consideration related to information security.

The organisation should establish at least two different levels of confidentiality of information (always within the organisation):

a ◆ What just a few members should know.

b ◆ What all members may know

This process may reduce the risk of confidential information leaking, whether by negligent behaviour and /or infiltration. It may also help the organisation see where is the leakage is coming from.

Might some aspects of our behaviour during our free time affect the image of our organisation?

- How do others see us?
- To what extent do other colleagues know what we do in our free time?

  What is the impact of the organisation image on security?
- ….

Summary

A defender at risk must care about security 24 hours a day, 7 days a week in all aspects of their lives, including during free time.

Free time needs proper consideration

The underlying question is always: "is there a security risk attached to..." If the answer is "no", then it is fine. If it is "yes", the issue needs to be explored and decisions taken about whether there are ways to fulfil a personal need within a protected environment or whether the need must be postponed until safer times or simply dropped as incompatible with the security needs of a human right defender.

All defenders' organisations at risk need a policy for the enjoyment of free time, from evenings to holidays. Special mention is necessary for the public use of alcohol and other drugs, how hidden relationships may interfere with security, and how organisational image about free time may affect security.

As free time involves risks, it is important not to forget to carry out thorough risk assessments.

ANNEX I

The UN Declaration on Human Rights Defenders.

UNITED NATIONS **A**

General Assembly

Distr.
GENERAL
A/RES/53/144
8 March 1999

Fifty-third session
Agenda item 110 *(b)*

RESOLUTION ADOPTED BY THE GENERAL ASSEMBLY

[on the report of the Third Committee (A/53/625/Add.2)]

53/144. Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms

The General Assembly,

Reaffirming the importance of the observance of the purposes and principles of the Charter of the United Nations for the promotion and protection of all human rights and fundamental freedoms for all persons in all countries of the world,

Taking note of Commission on Human Rights resolution 1998/7 of 3 April 1998[1], in which the Commission approved the text of the draft declaration on the right and responsibility of individuals, groups and organs of society to promote and protect universally recognized human rights and fundamental freedoms,

Taking note also of Economic and Social Council resolution 1998/33 of 30 July 1998, in which the Council recommended the draft declaration to the General Assembly for adoption,

Conscious of the importance of the adoption of the draft declaration in the context of the fiftieth anniversary of the Universal Declaration of Human Rights[2],

1. *Adopts* the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms, annexed to the present resolution;

[1] See Official Records of the Economic and Social Council, 1998, Supplement No. 3 (E/1998/23), chap. II, sect. A.

[2] Resolution 217 A (III).

2. *Invites* Governments, agencies and organizations of the United Nations system and intergovernmental and non-governmental organizations to intensify their efforts to disseminate the Declaration and to promote universal respect and understanding thereof, and requests the Secretary-General to include the text of the Declaration in the next edition of Human Rights: A Compilation of International Instruments.

85th plenary meeting
9 December 1998

Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms

The General Assembly,

Reaffirming the importance of the observance of the purposes and principles of the Charter of the United Nations for the promotion and protection of all human rights and fundamental freedoms for all persons in all countries of the world,

Reaffirming also the importance of the Universal Declaration of Human Rights[2] and the International Covenants on Human Rights[3] as basic elements of international efforts to promote universal respect for and observance of human rights and fundamental freedoms and the importance of other human rights instruments adopted within the United Nations system, as well as those at the regional level,

Stressing that all members of the international community shall fulfil, jointly and separately, their solemn obligation to promote and encourage respect for human rights and fundamental freedoms for all without distinction of any kind, including distinctions based on race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status, and reaffirming the particular importance of achieving international cooperation to fulfil this obligation according to the Charter,

Acknowledging the important role of international cooperation for, and the valuable work of individuals, groups and associations in contributing to, the effective elimination of all violations of human rights and fundamental freedoms of peoples and individuals, including in relation to mass, flagrant or systematic violations such as those resulting from apartheid, all forms of racial discrimination, colonialism, foreign domination or occupation, aggression or threats to national sovereignty, national unity or territorial integrity and from the refusal to recognize the right of peoples to self-determination and the right of every people to exercise full sovereignty over its wealth and natural resources,

Recognizing the relationship between international peace and security and the enjoyment of human rights and fundamental freedoms, and mindful that the absence of international peace and security does not excuse non-compliance,

Reiterating that all human rights and fundamental freedoms are universal, indivisible, interdependent and interrelated and should be promoted and implemented in a fair and equitable manner, without prejudice to the implementation of each of those rights and freedoms,

Stressing that the prime responsibility and duty to promote and protect human rights and fundamental freedoms lie with the State,

Recognizing the right and the responsibility of individuals, groups and associations to promote respect for and foster knowledge of human rights and fundamental freedoms at the national and international levels,

Declares:

2 Resolution 217 A (III).
3 Resolution 2200 A (XXI), annex.

Article 1

Everyone has the right, individually and in association with others, to promote and to strive for the protection and realization of human rights and fundamental freedoms at the national and international levels.

Article 2

1. Each State has a prime responsibility and duty to protect, promote and implement all human rights and fundamental freedoms, *inter alia*, by adopting such steps as may be necessary to create all conditions necessary in the social, economic, political and other fields, as well as the legal guarantees required to ensure that all persons under its jurisdiction, individually and in association with others, are able to enjoy all those rights and freedoms in practice.

2. Each State shall adopt such legislative, administrative and other steps as may be necessary to ensure that the rights and freedoms referred to in the present Declaration are effectively guaranteed.

Article 3

Domestic law consistent with the Charter of the United Nations and other international obligations of the State in the field of human rights and fundamental freedoms is the juridical framework within which human rights and fundamental freedoms should be implemented and enjoyed and within which all activities referred to in the present Declaration for the promotion, protection and effective realization of those rights and freedoms should be conducted.

Article 4

Nothing in the present Declaration shall be construed as impairing or contradicting the purposes and principles of the Charter of the United Nations or as restricting or derogating from the provisions of the Universal Declaration of Human Rights,2 the International Covenants on Human Rights3 and other international instruments and commitments applicable in this field.

Article 5

For the purpose of promoting and protecting human rights and fundamental freedoms, everyone has the right, individually and in association with others, at the national and international levels:

(a) To meet or assemble peacefully;

(b) To form, join and participate in non-governmental organizations, associations or groups;

(c) To communicate with non-governmental or intergovernmental organizations.

Article 6

Everyone has the right, individually and in association with others:

(a) To know, seek, obtain, receive and hold information about all human rights and fundamental freedoms, including having access to information as to how those rights and freedoms are given effect in domestic legislative, judicial or administrative systems;

(b) As provided for in human rights and other applicable international instruments, freely to publish, impart or disseminate to others views, information and knowledge on all human rights and fundamental freedoms;

(c) To study, discuss, form and hold opinions on the observance, both in law and in practice, of all human rights and fundamental freedoms and, through these and other appropriate means, to draw public attention to those matters.

Article 7

Everyone has the right, individually and in association with others, to develop and discuss new human rights ideas and principles and to advocate their acceptance.

Article 8

1. Everyone has the right, individually and in association with others, to have effective access, on a non-discriminatory basis, to participation in the government of his or her country and in the conduct of public affairs.

2. This includes, *inter alia*, the right, individually and in association with others, to submit to governmental bodies and agencies and organizations concerned with public affairs criticism and proposals for improving their functioning and to draw attention to any aspect of their work that may hinder or impede the promotion, protection and realization of human rights and fundamental freedoms.

Article 9

1. In the exercise of human rights and fundamental freedoms, including the promotion and protection of human rights as referred to in the present Declaration, everyone has the right, individually and in association with others, to benefit from an effective remedy and to be protected in the event of the violation of those rights.

2. To this end, everyone whose rights or freedoms are allegedly violated has the right, either in person or through legally authorized representation, to complain to and have that complaint promptly reviewed in a public hearing before an independent, impartial and competent judicial or other authority established by law and to obtain from such an authority a decision, in accordance with law, providing redress, including any compensation due, where there has been a violation of that person's rights or freedoms, as well as enforcement of the eventual decision and award, all without undue delay.

3. To the same end, everyone has the right, individually and in association with others, *inter alia*:

   (a) To complain about the policies and actions of individual officials and governmental bodies with regard to violations of human rights and fundamental freedoms, by petition or other appropriate means, to competent domestic judicial, administrative or legislative authorities or any other competent authority provided for by the legal system of the State, which should render their decision on the complaint without undue delay;

   (b) To attend public hearings, proceedings and trials so as to form an opinion on their compliance with national law and applicable international obligations and commitments;

   (c) To offer and provide professionally qualified legal assistance or other relevant advice and assistance in defending human rights and fundamental freedoms.

4. To the same end, and in accordance with applicable international instruments and procedures, everyone has the right, individually and in association with others, to unhindered access to and communication with international bodies with general or special competence to receive and consider communications on matters of human rights and fundamental freedoms.

5. The State shall conduct a prompt and impartial investigation or ensure that an inquiry takes place whenever there is reasonable ground to believe that a violation of human rights and fundamental freedoms has occurred in any territory under its jurisdiction.

Article 10

No one shall participate, by act or by failure to act where required, in violating human rights and fundamental freedoms and no one shall be subjected to punishment or adverse action of any kind for refusing to do so.

Article 11

Everyone has the right, individually and in association with others, to the lawful exercise of his or her occupation or profession. Everyone who, as a result of his or her profession, can affect the human dignity, human rights and fundamental freedoms of others should respect those rights and freedoms and comply with relevant national and international standards of occupational and professional conduct or ethics.

Article 12

1. Everyone has the right, individually and in association with others, to participate in peaceful activities against violations of human rights and fundamental freedoms.

2. The State shall take all necessary measures to ensure the protection by the competent authorities of everyone, individually and in association with others, against any violence, threats, retaliation, de facto or de *jure* adverse discrimination, pressure or any other arbitrary action as a consequence of his or her legitimate exercise of the rights referred to in the present Declaration.

3. In this connection, everyone is entitled, individually and in association with others, to be protected effectively under national law in reacting against or opposing, through peaceful means, activities and acts, including those by omission, attributable to States that result in violations of human rights and fundamental freedoms, as well as acts of violence perpetrated by groups or individuals that affect the enjoyment of human rights and fundamental freedoms.

Article 13

Everyone has the right, individually and in association with others, to solicit, receive and utilize resources for the express purpose of promoting and protecting human rights and fundamental freedoms through peaceful means, in accordance with article 3 of the present Declaration.

Article 14

1. The State has the responsibility to take legislative, judicial, administrative or other appropriate measures to promote the understanding by all persons under its jurisdiction of their civil, political, economic, social and cultural rights.

2. Such measures shall include, *inter alia*:

   (a) The publication and widespread availability of national laws and regulations and of applicable basic international human rights instruments;

   (b) Full and equal access to international documents in the field of human rights, including the periodic reports by the State to the bodies established by the international human rights treaties to which it is a party, as well as the summary records of discussions and the official reports of these bodies.

3. The State shall ensure and support, where appropriate, the creation and development of further independent national institutions for the promotion and protection of human rights and fundamental freedoms in all territory under its jurisdiction, whether they be ombudsmen, human rights commissions or any other form of national institution.

Article 15

The State has the responsibility to promote and facilitate the teaching of human rights and fundamental freedoms at all levels of education and to ensure that all those responsible for training lawyers, law enforcement officers, the personnel of the armed forces and public officials include appropriate elements of human rights teaching in their training programme.

Article 16

Individuals, non-governmental organizations and relevant institutions have an important role to play in contributing to making the public more aware of questions relating to all human rights and fundamental freedoms through activities such as education, training and research in these areas to strengthen further, *inter alia*, understanding, tolerance, peace and friendly relations among nations and among all racial and religious groups, bearing in mind the various backgrounds of the societies and communities in which they carry out their activities.

Article 17

In the exercise of the rights and freedoms referred to in the present Declaration, everyone, acting individually and in association with others, shall be subject only to such limitations as are in accordance with applicable international obligations and are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.

Article 18

1. Everyone has duties towards and within the community, in which alone the free and full development of his or her personality is possible.

2. Individuals, groups, institutions and non-governmental organizations have an important role to play and a responsibility in safeguarding democracy, promoting human rights and fundamental freedoms and contributing to the promotion and advancement of democratic societies, institutions and processes.

3. Individuals, groups, institutions and non-governmental organizations also have an important role and a responsibility in contributing, as appropriate, to the promotion of the right of everyone to a social and international order in which the rights and freedoms set forth in the Universal Declaration of Human Rights and other human rights instruments can be fully realized.

Article 19

Nothing in the present Declaration shall be interpreted as implying for any individual, group or organ of society or any State the right to engage in any activity or to perform any act aimed at the destruction of the rights and freedoms referred to in the present Declaration.

Article 20

Nothing in the present Declaration shall be interpreted as permitting States to support and promote activities of individuals, groups of individuals, institutions or non-governmental organizations contrary to the provisions of the Charter of the United Nations.

ANNEX II

COUNCIL OF
THE EUROPEAN UNION

Brussels, 9 June 2004
10056/1/04
REV 1
LIMITE
PESC 435
COHOM 17

NOTE

from:	Political and Security Committee
to:	Coreper/Council
Subject:	Draft Council Conclusions on EU Guidelines on Human Rights Defenders

1. At its meeting on 8 June, the Political and Security Committee discussed and finalised the above-mentioned draft Council Conclusions, which are reproduced in the Annex .
2. At its meeting on 1 June, the Political and Security Committee had endorsed the text « Ensuring Protection - European Union Guidelines on Human Rights Defenders » prepared in consultation with the Council Working Party on Human Rights (COHOM), which are now annexed to the draft Council Conclusions.
3. Coreper is invited to recommend that the Council approves these draft Council conclusions and the annexed Guidelines as an A-item at its meeting on 14/15 June.

ANNEX

Draft Council Conclusions

1. The Council welcomes and adopts the EU Guidelines on Human Rights Defenders (copy annexed). The Guidelines will be an integral part of the process of further strengthening the European Union's human rights policy in external relations. The Council notes that the Guidelines will enhance the European Union's activities in the protection and support of human rights defenders.
2. The Council notes that support for human rights defenders is already a long established element of the European Union's human rights external relations policy. The purpose of the Guidelines on Human Rights Defenders is to provide practical suggestions for enhancing EU action in relation to this issue. The Guidelines can be used in contacts with third countries at all levels as well as in multilateral human rights fora, in order to support and strengthen ongoing efforts by the Union to promote and encourage respect for the right to defend human rights. The Guidelines also provide for interventions by the Union for human rights defenders at risk and suggest practical means to support and assist human rights defenders.
3. The Council noted that while the Guidelines address the specific issues of Human Rights Defenders that they will contribute to reinforcing the EU's human rights policy in general.

Annex to the ANNEX

ENSURING PROTECTION
EUROPEAN UNION GUIDELINES ON HUMAN RIGHTS DEFENDERS

I. PURPOSE

1. Support for human rights defenders is already a long established element of the European Union's human rights external relations policy. The purpose of these Guidelines is to provide practical suggestions for enhancing EU action in relation to this issue. The Guidelines can be used in contacts with third countries at all levels as well as in multilateral human rights fora, in order to support and strengthen ongoing efforts by the Union to promote and encourage respect for the right to defend human rights. The Guidelines also provide for interventions by the Union for human rights defenders at risk and suggest practical means to support and assist human rights defenders. An important element of the Guidelines is support for the Special Procedures of the UN Commission on Human Rights, including the UN Special Representative on Human Rights Defenders and appropriate regional mechanisms to protect human rights defenders. The Guidelines will assist EU Missions (Embassies and Consulates of EU Member States and European Commission Delegations) in their approach to

human rights defenders. While addressing specific concerns regarding human rights defenders is their primary purpose, the Guidelines also contribute to reinforcing the EU's human rights policy in general.

II. DEFINITION

2. For the purpose of defining human rights defenders for these Guidelines operative paragraph 1 of the "UN Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognised Human Rights and Fundamental Freedoms" (see Annexe I), which states that "Everyone has the right, individually and in association with others, to promote and to strive for the protection and realisation of human rights and fundamental freedoms at the national and international levels" is drawn upon.
3. Human rights defenders are those individuals, groups and organs of society that promote and protect universally recognised human rights and fundamental freedoms. Human rights defenders seek the promotion and protection of civil and political rights as well as the promotion, protection and realisation of economic, social and cultural rights. Human rights defenders also promote and protect the rights of members of groups such as indigenous communities. The definition does not include those individuals or groups who commit or propagate violence.

III. INTRODUCTION

4. The EU supports the principles contained in the Declaration on the Right and responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognised Human Rights and Fundamental Freedoms. Although the primary responsibility for the promotion and protection of human rights lies with states, the EU recognises that individuals, groups and organs of society all play important parts in furthering the cause of human rights. The activities of human rights defenders include:
    - documenting violations;
    - seeking remedies for victims of such violations through the provision of legal, psychological, medical or other support; and
    - combating cultures of impunity which serve to cloak systematic and repeated breaches of human rights and fundamental freedoms.
5. The work of human rights defenders often involves criticism of government's policies and actions. However, governments should not see this as a negative. The principle of allowing room for independence of mind and free debate on a government's policies and actions is fundamental, and is a tried and tested way of establishing a better level of protection of human rights. Human rights defenders can assist governments in promoting and protecting human rights. As part of consultation processes they can play a key role in helping to draft appropriate legislation, and in helping to draw up national plans and strategies on human rights. This role too should be recognised and supported.
6. The EU acknowledges that the activities of Human Rights Defenders have over the years become more recognised. They have increasingly come to ensure greater protection for the victims of violations. However, this progress has been achieved at a high price: the defenders themselves have increasingly become targets of attacks and their rights are violated in many countries. The EU believes it is important to ensure the safety and protect the rights of human rights defenders. In this regard it is important to apply a gender perspective when approaching the issue of human rights defenders.

IV. OPERATIONAL GUIDELINES

7. The operational part of the Guideline is meant to identify ways and means to effectively work towards the promotion and protection of human rights defenders in third countries, within the context of the Common Foreign and Security Policy.

Monitoring, reporting and assessment

8. EU Heads of Mission are already requested to provide periodic reports on the human rights situation in their countries of accreditation. The Council Working Party on Human Rights (COHOM) has recently approved the outline of fact sheets to facilitate this task. In line with these fact sheets Missions should address the situation of human rights defenders in their reporting, noting in particular the occurrence of any threats or attacks against human rights defenders. In this contexts HoMs should be aware that the institutional framework can have a major impact on the ability of human rights defenders to undertake their work in safety. Issues such as legislative, judicial, administrative or other appropriate measures, undertaken by States to protect persons against any violence, threats retaliation, de facto or de jure adverse discrimination, pressure or any other arbitrary action as a consequence of his or her legitimate exercise of any of the rights referred to the UN Declaration on Human Rights Defenders are all relevant in this regard. Where it is called for, HoMs should make recommendations to COHOM for possible EU actions, including condemnation of threats and attacks against human rights defenders, as well as for demarches and public statements where human

rights defenders are at immediate or serious risk. HoMs should also report on the effectiveness of EU actions in their reports.

9. The HoMs reports and other relevant information, such as reports and recommendations from the Special Representative of the Secretary General for Human Rights Defenders, UN Special Rapporteurs and Treaty Bodies as well as non-governmental organisations, will enable COHOM and other relevant working parties, to identify situations where EU actions are called upon and decide actions to be taken or, where appropriate, make recommendations for such action to PSC / Council.

Role of EU Missions in supporting and protecting human rights defenders

10. In many third countries EU Missions (Embassies of EU Member States and European Commission Delegations) are the primary interface between the Union and its Member States and human rights defenders on the ground. They therefore have an important role to play in putting into practice the EU's policy towards human rights defenders. EU Missions should therefore seek to adopt a proactive policy towards human rights defenders. They should at the same time be aware that in certain cases EU action could lead to threats or attacks against human rights defenders. They should therefore where appropriate consult with human rights defenders in relation to actions which might be contemplated. Measures that EU Missions could take include:
    - co-ordinating closely and sharing information on human rights defenders, including those at risk;
    - maintaining, suitable contacts with human rights defenders, including by receiving them in Missions and visiting their areas of work, consideration could be given to appointing specific liaison officers, where necessary on a burden sharing basis, for this purpose;
    - providing, as and where appropriate, visible recognition to human rights defenders, through the use of appropriate publicity, visits or invitations;
    - attending and observing, where appropriate, trials of human rights defenders.

Promotion of respect for human rights defenders in relations with third countries and in multilateral fora

11. The EU's objective is to influence third countries to carry out their obligations to respect the rights of human rights defenders and to protect them from attacks and threats from non-state actors. In its contacts with third countries, the EU will, when deemed necessary, express the need for all countries to adhere to and comply with the relevant international norms and standards, in particular the UN Declaration. The overall objective should be to bring about an environment where human rights defenders can operate freely. The EU will make its objectives known as an integral part of its human rights policy and will stress the importance it attaches to the protection of human rights defenders. Actions in support of these objectives will include:
    - where the Presidency, or the High Representative for the CFSP or EU Special Representatives and Envoys, or European Commission are making country visits they will, where appropriate, include meetings with, and raising individual cases of, human rights defenders as an integral and part of their visits to third countries;
    - the human rights component of political dialogues between the EU and third countries and regional organisations, will, where relevant, include the situation of human rights defenders. The EU will underline its support for human rights defenders and their work, and raise individual cases of concern whenever necessary;
    - working closely with other like minded countries with similar views notably in the UN Commission on Human Rights and the UN General Assembly;
    - promoting the strengthening of existing regional mechanisms for the protection of human rights defenders, such as the focal point on human rights defenders of the African Commission on Human and Peoples' Rights and the special Human Rights Defenders Unit within the Inter-American Commission on Human Rights, and the creation of appropriate mechanisms in regions where they do not exist.

Support for Special Procedures of the UN Commission on Human Rights, including the Special Representative on Human Rights Defenders

11. The EU recognises that the Special Procedures of the UN Commission on Human Rights (Special Rapporteurs, Special Representatives, Independent Experts and Working Groups) are vital to international efforts to protect human rights defenders because of their independence and impartiality; their ability to act and speak out on violations against human rights defenders worldwide and undertake country visits. While the Special Representative for Human Rights Defenders has a particular role in this regard the mandates of other Special Procedures are also of relevance to human rights defenders. The EU's actions in support of the Special Procedures will include:
    - encouraging states to accept as a matter of principle requests for country visits by UN Special Procedures;

- promoting via EU Missions, the use of UN thematic mechanisms by local human rights communities and human rights defenders including, but not limited to facilitating the establishment of contacts with, and exchange information between, thematic mechanisms and human rights defenders;
- since the Special Procedures are unable to carry out their mandate in the absence of adequate resources, EU Member States will support the allocation of sufficient funds from the general budget to the Office of the High Commissioner for Human Rights

Practical supports for Human Rights Defenders including through Development Policy

13. Programmes of the European Community and Member States aimed at assisting in the development of democratic processes and institutions, and the promotion and protection of human rights in developing countries are among a wide range of practical supports for assisting human rights defenders. These can include but are not necessarily limited to the development co-operation programmes of Member States. Practical supports can include the following:
    - bi-lateral human rights and democratisation programmes of the European Community and Member States should take further account of the need to assist the development of democratic processes and institutions, and the promotion and protection of human rights in developing countries by, inter alia, supporting human rights defenders through such activities as capacity building and public awareness campaigns;
    - by encouraging and supporting the establishment, and work, of national bodies for the promotion and protection of human rights, established in accordance with the Paris Principles, including, National Human Rights Institutions, Ombudsman's Offices and Human Rights Commissions.
    - in the establishment of networks of human rights defenders at an international level, including by facilitating meetings of human rights defenders;
    - seeking to ensure that human rights defenders in third countries can access resources, including financial, from abroad;
    - by ensuring that human rights educations programmes promote, inter alia, the UN Declaration on Human Rights Defenders.

Role of Council Working Parties

14. In accordance with its mandate COHOM will keep under review the implementation and follow-up to the Guidelines on Human Rights Defenders in close co-ordination and co-operation with other relevant Council Working Parties. This will include:
    - promoting the integration of the issue of human rights defenders into relevant EU policies and actions;
    - undertaking reviews of the implementation of the Guidelines at appropriate intervals;
    - continuing to examine, as appropriate, further ways of co-operating with UN and other international and regional mechanisms in support of human rights defenders.
    - Reporting to Council, via PSC and COREPER, as appropriate on an annual basis on progress made towards implementing the Guidelines.

Annex I to Annex to the ANNEX
(UN Declaration on HRD)

Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms

Annex II to Annex to the ANNEX

Relevant international instruments

- The Universal Declaration of Human Rights
- The International Covenant on Civil and Political Rights
- The International Covenant on Economic, Social and Cultural Rights
- The Convention Against Torture and other Cruel, Inhuman or Degrading Treatment or Punishment
- The Convention on the Rights of the Child
- The Convention on the Elimination of Discrimination Against Women
- The Convention on the Elimination on all Forms of Racial Discrimination
- The European Convention on Human Rights, its protocols and the relevant case law of the European Court of Human Rights
- European Social Charter / Revised European Social Charter
- African Charter for Human and Peoples' Rights
- American Convention on Human Rights
- Geneva Conventions on the Protection of Victims of War and its Protocols as well as customary rules of humanitarian law applicable in armed conflict
- The 1951 Convention regarding the Status of Refugees and its 1967 Protocol
- The Rome Statute of the International Criminal Court
- Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms.

ANNEX III

PI advocacy recommendations for HRD related to EU Missions, EU Members States Embassies and Special EU representatives (more tips on www.protectionline.org)

Since the adoption of the UN Declaration, the following mechanisms have been established to protect defenders worldwide:

- The mandate of **United Nations Special Representative of the Secretary General on Human Rights Defenders**, created by the UN Commission on Human Rights.
- The mandate of **Special Reporter of the African Commission on Human and People's Rights.**
- **Resolution on the protection of human rights defenders in Africa from** the African Commission on Human and Peoples' Rights (ACHPR) meeting at its 35th ordinary session held from 21st May to 4th June 2004, in Banjul, the Gambia.
- The **Human Rights Defenders Unit of the Inter-American Commission on Human Rights**.
- The **EU** has also adopted specific **Guidelines on Human Rights Defenders** as a tool that EU missions should implement to protect defenders in third countries.
- **Council of Europe**: Adoption of the Declaration of the Committee of Ministers for enhanced protection of human rights defenders **February 18, 2008**.
- Asian Human Rights Commission

In 2004, the EU Council of Ministers adopted the EU Guidelines on Human Rights Defenders. The EU Guidelines reiterate the UN Declaration on HRD and direct specific recommendations to all EU Missions and EU Members States. EU recommendations aim at:

- adopting proactive policies for the protection of HRDs
- Using diplomatic avenues to obtain, from local and national governments of the HRDs affected, the commitment to the full respect of the HRD rights.

The EU Guidelines can also be obtained from EU Desks and Members States embassies.

The EU Missions (EU Member States Embassies and EU Commission Delegations) constitute the first point of contact between the EU, EU Member States and the local HRDs)

PI therefore recommends that HRD at the very least:

- ask for the EU Guidelines to be translated into the HRDs' language and distributed to HRD organisations and national and local authorities
- send regular information updates about their situation to the EU Heads of Mission (HoM) and to national and international NGOs in order to raise awareness and increase coordination between stakeholders

- maintain regular contact with EU Missions so that local HRDs can be informed about the EU Guidelines and the EU Mission initiatives for the protection of HRDs. This regular contact will allow EU Missions to be kept informed about both the situation of HRDs and their reported recommendations on the protection and support measures to be taken..
- ask for EU Missions to share and implement consistent practice in protection and medium-term strategies
- invite HoM or HR officers to visit area of work of HRD especially where HRDs are at particular risk (for instance, in conflict areas or places where HRDs have been already attacked or threatened)
- request urgent action when HRD defenders are threatened or arrested
- request safe places and full assistance to HRD at risk
- solicit or accept invitations and promotion from EU Missions once HRDs have carried out a risk assessment on the impact of their profile possibly being raised. Highlight possible consequent security issues and request protection support. Request assistance and observation by EU HoM in the event of trials against HRDs. This can guarantee a fair trial but a presence is required throughout the proceedings (from the reading of the indictment to the reading of the sentence) in order to guarantee independence. Ask for the observers to communicate with the HRD under trial. Ask for EU observers also to be present at trials against HR violators in order to avoid impunity for their crimes.
- be updated on visits to the HRD country by the EU Presidency, CFSP - Common Foreign and Security Policy High Representative, EU Special Representatives or EU Commission Members, and request meetings with them.
- ask for the situations of HRDs to be included in the agenda of political dialogue between EU, and the HRDs' country and regional organisations.
- ask for coordinated political actions with other stakeholders, particularly with the UN Human Rights Council and the UN General Assembly. Ask for coordination with existing regional bodies for the protection of HR and HRD such as the African Commission on Human and Peoples' Rights, the Defenders' Unit of the Inter-American Commission on Human Rights, the Asian Human Rights Commission.
- ask for the EU Heads of Mission (HoM) reports to be public and accessible to HRDs

Fundraising

HRDs can fundraise directly with embassies (HR Programmes) and with the EU via the European Instrument for Democracy and Human Rights (EIDHR). EIDHR allows the European Commission to fund NGOs without the approval of the Government of the third country. **http://ec.europa.eu/europaid/projects/eidhr/index_en.htm** or simply EIDHR. More information about other financial instruments available through the same link.

Furthermore:

Although the EU Guidelines cover EU missions, EU Institutions and EU Member States and their Embassies, HRDs should remember that support can also be sought via other diplomatic corps and international organisations as the UN Declaration on HRDs can be used with all stakeholders.

Bibliography and additional resources

Bibliography

- Amnesty International (2003): "Essential actors of our time. Human rights defenders in the Americas". AI International Secretariat (Index AI: AMR 01/009/2003/s)
- AVRE and ENS (2002): "Afrontar la amenaza por persecuci_n sindical". Escuela de Liderazgo Sindical Democr_tico. Published by the Escuela Nacional Sindical and Corporaci_n AVRE. Medell_n, Colombia.
- Bettocchi, G., Cabrera, A.G., Crisp, J., and Varga, A (2002): "Protection and solutions in situations of internal displacement". EPAU/2002/10, UNHCR.
- Cohen, R. (1996): "Protecting the Internally Displaced". World Refugee Survey.
- Conway, T., Moser, C., Norton, A. and Farrington, J. (2002) "Rights and livelihoods approaches: Exploring policy dimensions". DFID Natural Resource Perspectives, no. 78. ODI, London.
- Dworken, J.T "Threat assessment". Series of modules for OFDA/InterAction PVO Security Task Force (Mimeo, included in REDR Security Training Modules, 2001).
- Eguren, E. (2000): "Who should go where? Examples from Peace Brigades International", in "Peacebuilding: a Field Perspective. A Handbook for Field
- Diplomats", by Luc Reychler and Thania Paffenholz (editors). Lynne Rienner Publishers (London).
- Eguren, E. (2000), "The Protection Gap: Policies and Strategies" in the ODI HPN Report, London: Overseas Development Institute.
- Eguren, E. (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/a060.pdf**
- Eriksson, A. (1999) "Protecting internally displaced persons in Kosovo". **http://web.mit.edu/cis/www/migration/kosovo.html#f4**
- Lebow, Richard Ned and Gross Stein, Janice. (1990) "When Does Deterrence Succeed And How Do We Know?" (Occasional Paper 8). Ottawa: Canadian Inst. for Peace and International Security.
- Mahony, L. and Eguren, E. (1997): "Unarmed bodyguards. International accompaniment for the protection of human rights". Kumarian Press. West Hartford, CT (USA).
- Martin Beristain, C. and Riera, F. (1993): "Afirmaci_n y resistencia. La comunidad como apoyo". Virus Editorial. Barcelona.

- Paul, Diane (1999): "Protection in practice: Field level strategies for protecting civilians from deliberate harm". ODI Network Paper no. 30.
- SEDEM (2000): Manual de Seguridad.. Seguridad en Democracia. Guatemala.
- Sustainable Livelihoods Guidance Sheets (2000). DFID. London, February 2000
- Sutton, R. (1999) The policy process: An overview. Working Paper 118. ODI. London.
- UNHCHR (2004): "About Human Rights Defenders" (extensive information): http://www.unhchr.ch/defenders/about1.htm
- UNHCHR (2004): "Human Rights Defenders: Protecting the Right to Defend Human Rights". Fact Sheet no. 29. Geneva.
- UNHCHR (2004): On women defenders: **www.unhchr.ch/defenders/tiwomen.htm**
- UNHCR (1999): Protecting Refugees: A Field Guide for NGO. Geneva.
- UNHCR (2001): Complementary forms of protection. Global Consultations on International Protection. EC/GC/01/18 4 September 2001
- UNHCR (2002) Strengthening protection capacities in host countries. Global Consultations on International Protection. EC/GC/01/19 * / 19 April 2002
- UNHCR-Department of Field Protection (2002) Designing protection strategies and measuring progress: Checklist for UNHCR staff. Mimeo- Geneva.
- Van Brabant, Koenraad (2000): "Operational Security Management in Violent Environments". Good Practice Review 8. Humanitarian Practice Network. Overseas Development Institute, London.

Additional resources

Protection International-PI- provides trainings and consultancy on risk assesment, protection and security for human rights defenders since 2000. Please contact: pi@protectioninternational.org or write to: PI, Rue de la Linière, 11 - 1060 Brussels (Belgium)

Tel: + 32 (0)2 609 44 05 +32 (0)2 609 44 07

Fax: +32 (0)2 609 44 06

www.protectioninternational.org

www.protectionline.org

Tactical Technology Collective: **www.tacticaltech.org** (since 2003 - technical expertise in digital security): "NGO in a Box".

Index of Chapters

Thematic Index

Luis Enrique Eguren

(Spain), physician and expert in protection, member of the Research and Training Unit of Protection International. He has worked with PBI in El Salvador, Sri Lanka and Colombia, as well as in short missions in other countries with other international organisations. Consultant, trainer and researcher, he has published several articles and books on the topic of protection.

© Maria Dermitzaki

Marie Caraj

Interpreter and expert in protection. Member of the Research and Training Unit of Protection International. She worked with PBI and PBI-BEO (1985-2007). Succession of short missions in Africa, Asia, Latin America Consultant, trainer and researcher.

"(...) the gravity of the risks faced on a daily basis by human rights defenders is such that it is also important to pursue other means to strengthen their protection. In this regard I hope that this Protection Manual will support human rights defenders in developing their own security plans and protection mechanisms. Many human rights defenders are so engaged by their work to protect others that they give insufficient attention to their own security. It is important that all of us involved in working for human rights understand that we must be concerned about security for ourselves and for the people we work with and for."

(Hina Jilani, Former UN Secretary-General's Special Representative on Human Rights Defenders)

"Since we've had this training, lots of things have changed in our organisation, just because most of the things we learned about on the course was stuff we obviously didn't know about before. Now, we're stronger because of this training, and we know much better how to assess the risks we're running on a day to day basis, as well as how to judge security incidents, threats and the likelihood of them being carried out."

"(...) Your active teaching methods are really inclusive, and that's a big plus as it let us exchange information. We are sure that the results will give us lots of insights".

"I felt I got a really good quality training in how to be a real human rights defender. I'm going to change the way I work after this."

(Defenders in the Democratic Republic of Congo)

"Congratulations to the efforts and format since it was really instructive and helped us find our way around our daily situation."

(A defender in Guatemala)

"I learned loads about a world I've known about for a long time, but that I'd hardly ever looked at in that way before."

(A defender in Mexico)

"(...) It is a very new topic for me. Though we are working in such a field where there is always a threat to our security, we never thought of the need of such training or never had the time to think for our security but after this training I personally felt that it should be kept at the top most level before launching any programme. In other words this training is really essential for all."

(A defender in Nepal)

PROTECTION international

With the support of BMZ and SPF AE

Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung

SERVICE PUBLIC FÉDÉRAL AFFAIRES ETRANGÈRES BELGIQUE

The New Protection Manual for Human Rights Defenders was researched and written by Enrique Eguren and Marie Caraj, at the Research and Training Unit of Protection International.

Protection International, Rue de la Linière, 11. B-1060 Brussels
Tel: +32(0)2 609 44 05 / +32(0)2 609 44 07, Fax: +32(0)2 609 44 07
E-mail pi@protectioninternational.org www.protectioninternational.org

One-stop website on protection for human rights defenders: www.protectionline.org