WORKBOOK ON SECURITY:

PRACTICAL STEPS FOR HUMAN RIGHTS DEFENDERS AT RISK

FRONT LINE DEFENDERS

WORKBOOK ON SECURITY:

PRACTICAL STEPS FOR HUMAN RIGHTS DEFENDERS AT RISK

FRONT LINE DEFENDERS

Published by Front Line 2011

Front Line
Grattan House, 2nd Floor
Temple Road
Blackrock
Co Dublin
Ireland
Phone: +353 1 212 3750
Fax: +353 1 212 1001

Cover illustration: Dan Jones

Copies of this Workbook are available free online at **www.frontlinedefenders.org**
(and will be available in English, Arabic, French, Russian and Spanish)

To order a Workbook, please contact:
workbook@frontlinedefenders.org

or write to us at the above address
Price: €20 plus post and packing

ISBN: 978-0-9558170-9-0

Disclaimer:
Front Line does not guarantee that the information contained in this Workbook is foolproof or appropriate to every possible circumstance and shall not be liable for any damage incurred as a result of its use.

Written by Anne Rimmer, Training Coordinator, Front Line and reviewed by an invaluable team of human rights defenders: Usman Hamid, International Centre for Transitional Justice and Kontras, Indonesia, Ana Natsvlishvili, Georgia and a HRD from the Middle East (name withheld for security reasons).

Acknowledgements:
This Workbook is based on the concepts introduced in the Protection Manual for Human Rights Defenders, Enrique Eguren/PBI BEO, and the updated New Protection Manual for Human Rights Defenders, Enrique Eguren and Marie Caraj, Protection International. We are grateful to Protection International for permission to reproduce extracts from the New Protection Manual for Human Rights Defenders.

We are deeply grateful for inputs from other security specialists and the contributions of HRDs working in difficult environments who have discussed risks with us and shared their survival strategies.

TABLE OF CONTENTS

PREFACE

"Great challenges lie ahead of us. Our work as human rights defenders is humanitarian and in the public interest: we work to protect life, dignity and the future of our people.

Dr Yuri Giovanni Melini

We have seen repression and violence at first hand. It has sometimes forced us to demonstrate our physical strength and, on occasion, has even required a life to be sacrificed for the benefit of others. We do this because we have principles and values, because we love life in all its forms and because we demand the respect we deserve from the state and its institutions, from governments and governors. We do this because it is right, and not because it is financially rewarding.

This Workbook on the protection of human rights defenders is an opportunity to reflect on the fact that our work is essential. It allows people, groups, populations, societies and nations to express themselves, demand their rights and denounce the violation of what they are entitled to.

As we go about our daily tasks, following good safety practices will ensure our safety and that of our collaborators and families. If we use the information contained in this manual to draw up simple, yet vital, personal and organisational safety plans, it will enable us to work harder and further for human rights, and indeed for humankind.

Safe from fear, with courage, humility and determination, the future is ours to take. Never take a step backwards, not even if it's to push yourself forward."

Dr Yuri Giovanni Melini
Director General
Centro de Acción Legal-Ambiental y Social de Guatemala - CALAS
(Centre of Legal Action in Environment and Social issues)
GUATEMALA
Winner of Front Line Award for Human Rights Defenders at Risk 2009

"Front Line addresses the safety and protection of human rights defenders, especially women human rights defenders, in its programmes.

Human rights defenders need new strategies that are inspired by a theory of security and human rights, of dignity, freedom and justice. This Workbook, created with a view to protecting human rights defenders, is aimed at them.

It aims to draw attention to specific situations arising from the activities carried out by human rights defenders, to prepare them to deal with the inconveniences, unexpected risks, threats and security incidents they may meet. It also seeks to prevent these situations and to deal with stress and insecurity.

Having made use of such strategies ourselves, we believe that they have positively influenced

the lives of the human rights defenders, even if it cannot be claimed that they hold the response to all problems that arise from the work of human rights defenders and women human rights defenders, such as the psychological issues, underlying emotional difficulties and danger and discord that can arise between the various actors in the field... We welcome this document, another Front Line publication dedicated to the safety and well-being of human rights defenders."

Gégé Katana Bukuru

Gégé Katana Bukuru
Executive Secretary
Solidarité des Femmes Activiste pour la defense des droits de l'homme - SOFAD
(Solidarity Movement of Women Human Rights Activists)
DEMOCRATIC REPUBLIC OF CONGO
Winner of Front Line Award for Human Rights Defenders at Risk 2007

"The Joint Mobile Group (JMG) has been working in the Chechen Republic since November 2009. This group consists of members of different Russian human rights organisations; it was created in order to receive credible and proven information relating to human rights violations in the Chechen Republic. In addition, the group's task is to reveal the causes for ineffective investigations by the investigative authorities into cases of torture and abductions in Chechnya.

Joint Mobile Group

Our activities wouldn't be successful without taking serious security measures. The existence of a system of such measures in our everyday activity permits us to work efficiently in this complicated region of Russia for 18 months.

Security measures of the JMG include those ideas developed by the specialists of Front Line. That is why we are delighted to welcome this manual on security and protection for human rights defenders. It's crucial for any human rights activist facing risks to have a fine security plan."

Joint Mobile Group
RUSSIA
Winner of Front Line Award for Human Rights Defenders at Risk 2011

DEDICATION

This Workbook is dedicated to all those Human Rights Defenders at risk with whom Front Line has worked.

Many HRDs have openly shared the risks they faced, their fears, their dilemmas about balancing security with effectiveness, and the creative strategies they employ in order to continue their invaluable work.

Our work, and our lives, have been enriched and inspired by knowing them.

CHAPTER 1: INTRODUCTION

> ***"I used to think security planning was only for those human rights defenders who weren't brave enough to face the risks. Now I realise that doing this planning makes you stronger and more effective."*** **HRD, Africa**

This Chapter introduces Human Rights Defenders (HRDs) and some of the risks faced by defenders. It gives a brief overview of steps for producing a security plan, and gives the definitions of security, protection and safety we will use in this Workbook. At the end there is a short exercise for you to do in relation to your own security.

Welcome

Welcome to the Workbook on Security: Practical Steps for Human Rights Defenders (HRDs) at Risk.

HRDs are those who work non-violently on behalf of others for any or all of the rights enshrined in the Universal Declaration of Human Rights. This includes those who work for civil and political rights, social, economic, environmental and cultural rights, and the right to equality, such as those working for women's rights and Lesbian, Gay, Bisexual, Transgender and Intersex (LGBTI) rights.

Some examples of HRDs are: a group running a legal aid clinic; an organisation which documents torture (including rape) and assists the survivors; those working for the rights of disadvantaged communities such as women or bonded labour; anti-corruption activists; workers at women's shelters; indigenous leaders advocating for the rights of their communities; protesters against environmental damage; those working for the right to express sexual identity and orientation. Sometimes these HRDs have been victims themselves and then begin working for others, for example a wife whose husband has disappeared who organises other family members to work to bring the perpetrators of disappearances to justice. Sometimes HRDs work in human rights organisations, sometimes they work alone.

HRDs all over the world may face risks because of the work that they do. These risks may include assault, torture – including sexual torture, imprisonment, and even assassination. The perpetrators may be military or police officers or their intelligence operatives, multi-national corporations, armed opposition groups, local militia, local criminals hired by others, conservative religious groups, community members, or even members of the families of HRDs.

Whatever the risks, whoever the perpetrators, wherever the danger arises, there are ways to reduce the threats and mitigate the impact of any attack.

> *"We mapped all the resources available to us in the NGO arena – the legal aid clinics, independent media, psychological support... Now we know who we can call on when we need help."*
> HRD, Eastern Europe

Steps to producing a security plan

This Workbook has been inspired by the hundreds of HRDs from over 50 countries who have attended Front Line's workshops on security and protection. These HRDs have been able to continue their work because they have taken steps to manage their security. They have assessed their situation in a systematic way and developed strategies and tactics which best suit their unique environment. The Workbook is based on the *Protection Manual for Human Rights Defenders*[1], discussions with security specialists, and the contributions from workshop participants and other HRDs on-the-ground in difficult environments who have discussed risks with us and shared their survival strategies.

1. "Protection Manual for Human Rights Defenders", Enrique Eguren/PBI BEO, published by Front Line 2005 and available on the Front Line website www.frontlinedefenders.org

The Workbook takes you through the steps to producing a security plan – for yourself and for your organisation (for those HRDs who are working in organisations). It follows a systematic approach for assessing your security situation and developing risk and vulnerability reduction strategies and tactics.

The steps include:

- Context analysis
- Assessing risk
- Analysing threats
- Producing security plans
- Implementing and reviewing plans

We know from working with HRDs in countries around the world that there is usually a very high workload and limited resources. Steps to manage security can sometimes be put to one side because there never seems to be enough time, or because HRDs think they must consider the people they work for rather than themselves. However, HRDs who have invested time and energy in developing the capacity to manage their security tell us that it is worth it, both because it can reduce the threat of human rights work being disrupted by a security incident and because it reduces stress and assists people to be more effective in their work.

We have included a chapter on stress and wellbeing in the Workbook. This is because HRDs tell us that they experience huge amounts of stress due to many factors, including workload, expectations, threats, and traumatic experiences. Being stressed can considerably reduce your ability to be secure and lead to burnout. We hope this chapter will help you to manage your stress better.

"If a HRD is targeted, we mobilise all the other human rights activists in the country to develop a web of support. Anyone who meets an international visitor or other influential person talks about this person at risk. This raises their profile enormously, and reduces their vulnerability."
HRD, Eastern Europe

Going through this Workbook will take some time, but it is not meant to be a theoretical piece of work. It is designed to raise your awareness about security issues and to help you consider how to mitigate threats.

Along the way we have included examples of simple tactics that HRDs have used to make themselves more secure. We hope these examples – whilst not necessarily being directly relevant to your own unique situation – will inspire you to think creatively about how to reduce the risks you face so that you can continue the essential work you do in the safest possible way.

"Is security an absence of risk? Or being able to manage risk? Obviously by choosing to be a HRD working for the rights of other people, individuals and organisations have taken on certain risks. These will vary from country to country and context to context and will vary over time. Defenders have an obligation to themselves and the communities on whose behalf they work to pay attention to security. It is not a question of being self-interested but of ensuring the continuation of the work on behalf of others. It is about caring for the victims even more. "It is not a luxury, it is a necessity." HRD, Europe

Important notes

No book can **tell** you how to make yourself secure. Advice is rarely applicable to all the HRDs under threat all over the world. Different circumstances require different responses, and the same circumstances involving different people also may require varied strategies. While there are examples and check lists in this Workbook, they are included for illustration and to stimulate your own ideas about what is required to improve your security, and are not intended in any way as blueprints.

Security management is partly about setting up procedures. But procedures will only be effective if they are an appropriate response to the risks you face. The challenge, therefore, is to identify correctly the threats and vulnerabilities in your environment at any given time and supplement this assessment by constant situational awareness.

As different people face different risks, it is important for you to consider which of your personal attributes may make you more vulnerable to risks. In most societies women Human Rights Defenders (WHRD) and Lesbian, Gay, Bisexual, Transgender, Intersex (LGBTI) HRDs face additional risks because of who they are and how they express themselves. In this Workbook issues of identity and orientation are integrated, rather than dealt with in separate sections.

Although technology brings many benefits to HRDs (easy communication by mobile phone, fast dissemination of information through email, networking through social networks etc) it also brings the risk of surveillance and interference by those opposed to your work. This Workbook is not intended to be a technical guide to digital security – for this we refer you to *Security in-a-box, Tactical Technology Collective & Front Line* - **https://security.ngoinabox.org/** and Mobile in-a-box **http://mobiles.tacticaltech.org/**

Security-in-a-box

However, you will find some basic advice in two of the appendices – Appendix 14 on Computer and Phone security and Appendix 15 on Surveillance technology and methodology.

The examples used in this Workbook are anonymous for reasons of privacy and security – the names have been changed and in some circumstances the experiences of more than one HRD have been amalgamated.

Definitions

This Workbook is focussed on HRDs and the measures that can be taken to enhance their personal and organisational security. HRDs also need to be concerned about the safety and security of the people they work for and with (clients, witnesses etc), and many of the security measures identified here will benefit them too.

The Workbook deals with:

Security: freedom from risk or harm resulting from violence or other intentional acts

and

Protection: measures taken by HRDs or other actors to enhance security

It does not aim to deal comprehensively with:

Safety: freedom from risk or harm as a result of unintentional acts (accidents, natural phenomena, illness).

However, it is worthwhile to spend some time considering which threats to your safety are high risk because of your environment, work practices or lifestyle, and require risk mitigation action on your part. (Note that people are more likely to underestimate the dangers of common risks, eg vehicle accidents, and overestimate the less common risks, such as flying.)

Activity: Considering your own security situation

We hope this Introduction has stimulated your thinking about your security situation. On the following pages you may wish to list your initial thoughts about the factors which make you feel more secure and the factors which make you feel less secure. (Some people may prefer to draw or map these factors.)

"After assessing our overall security and safety, we realised a big threat was the location of our office, which is in the path of an avalanche. We decided to move."
HRD, Asia

"Vehicle accidents are very common in our country. We made a rule that staff should not drive in the dark except in extreme circumstances."
HRD, Africa

This information can be used when you are drawing up a personal security plan.

Note: All the exercises you fill in with personal details in this Workbook are on sheets which can be torn out of this publication, which you may want to keep in a separate, safe place.

"WHAT FACTORS MAKE ME FEEL SECURE?"

ACTIVITY

"WHAT FACTORS MAKE ME FEEL INSECURE?"

ACTIVITY

CHAPTER 2: RISK ASSESSMENT

> ***"We can't avoid risks as defenders, but we have the responsibility to take time to manage them"*** **HRD, Americas**

This Chapter looks at some of the risks faced by HRDs. It introduces the Risk Formula - a tool that assists you to identify the different components that increase or reduce your risk. There is a case study based on the Risk Formula for you to consider. Then there is an exercise so you can complete your own Risk Assessment. There is also an explanation of the Risk Matrix, which uses the concepts of probability and impact to assist you to assess the most important risks you face.

"A human rights journalist was denounced by the President as a traitor. All the other journalists wrote articles defending him and this helped protect him".
HRD, Middle East

"I was having a meeting with an Ambassador in his embassy when I got a call to say that armed thugs had surrounded our office. The Ambassador came with me to the office and when the thugs saw who I was with, they retreated."
HRD, Asia

"I was threatened all the time that I would lose my job if I didn't stop my human rights work. I set up my own business so these threats would have no impact."
HRD, Eastern Europe

Introduction

What you do as a HRD can challenge the interests of powerful actors and this can put you at great risk. The more effective your work is, the more likely it is that this will put you at risk. Defenders in many countries throughout the world face risks because of their work.

The challenge is to be able to assess – as far as possible – the degree of risk, and take actions to minimise this risk.

Assessment of risk will be based on your unique context. Understanding your context is the prerequisite for being able to take effective security measures. We include a chapter on this topic at the end of this Workbook (Chapter 6: Understanding your context). While such a chapter would normally be at the beginning of publications on security, HRDs have advised us that - because the exercises may not be as easy to begin immediately - it is better to start with the more immediate issue of risk.

Risks

Risks will differ according to the context of your country, the patterns of threats and attacks, the perpetrators, the degree of impunity, and the individual's identity, profile, activities and location. In many countries, WHRD and LGBTI HRDs are more at risk than others; HRDs working in the rural areas with fewer resources and without close access to protective allies or institutions are also often more at risk. However, many risks faced by HRDs are of a similar nature, such as:

- Stigmatisation of HRDs as 'anti-state', 'anti-religious', 'agents of Western powers', 'members of armed opposition groups', 'sex workers', 'traffickers', 'corrupt'.....the list is endless.
- Interference with travel, writing or associating with others
- Blackmail (eg "if you don't stop your activities, your son will be arrested")
- Being targeted with Administrative measures – such as requirements to provide extensive financial information, proof of ownership of legitimate computer software, difficulties in registering or re-registering organisations
- Physical and sexual assaults (by personnel or by devices such as bombs)
- Attacks on livelihood – losing job or education opportunities
- Attacks on property – vehicle, house or office vandalised or destroyed

Nabeel Rajab, Bahrain with tear gas canisters fired on his home

- Detention / arrest / imprisonment - perhaps based on false or spurious accusations, or civil or criminal cases on defamation
- Ill-treatment / torture
- Abduction / kidnap
- Murder

The perpetrators might be the authorities, companies, powerful groups or sections of the community.

This list may appear intimidating, but there are ways to minimise the risks. To begin this, we will look at a tool which is at the heart of this Workbook – the Risk Formula.

The Risk Formula

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

The **definitions** for the terms are:

RISK – the possibility of events that result in harm

THREAT – declaration or indication of an intention to inflict damage, punish or hurt (recent or immediate)

CAPACITY – any resource (including abilities and contacts) which improve security

VULNERABILITY – any factor which makes it more likely for harm to materialise or result in greater damage

This may look complicated, but let us look at a true story of a HRD at risk to identify the different components.

Role play of attack by armed men on a WHRD, illustrating a security plan in action

Activity
While you are reading it, make notes on what were the risks Juan faced, the threats, the vulnerabilities and the capacities.

Juan, an LGBTI HRD in the Americas, knew that there was a lot of hostility in the community towards his organisation's work and him personally. One day he was walking in town and saw two men pointing at him and appearing to talk about him. Juan became alert to a potential risk.

In his head he had a 'map' of the town, knowing where his friends and sympathisers were located. He quickly walked to a nearby shop where the shopkeeper was a friend of his.

Juan and the shopkeeper saw a mob start forming on the other side of the street. The shopkeeper locked the door and pulled down the metal shutter. Juan had his mobile phone with him, charged and with credit. He rang a contact of his (his emergency security contact, who had been prepared for such a scenario) – he had inserted the number as a speed-dial number on his phone.

His emergency security contact rang the local police (who could be relied on to help the HRD, due to previous advocacy work) immediately.

The police arrived and rescued Juan just as the mob was starting to break the door down.

Risks . . . . . .
Threats . . . . . .
Vulnerabilities. . . . . .
Capacities . . . . . .

Check these with our assessment:

Risks:
- assault / torture (including sexual assault)
- murder

(There are also risks for the shopkeeper and the shop premises)

Threats: it is useful to look at the threats at 3 different levels -
1) the 2 men pointing and talking about Juan. This can be called a 'security incident' (an event which could indicate a threat or lead to one) – it could be that the men were just admiring Juan's jeans! At this stage it wasn't clear.
2) the mob forming across the street
3) the mob attacking the shop

Vulnerabilities:
- antagonistic community
- known personally as an LGBTI HRD
- alone
- walking

Capacities:
- mobile phone, charged, with credit, emergency contact number on speed-dial
- friends and allies: the shopkeeper; the emergency contact; the police
- advance planning – 'map' of the town
- psychological aspect – keeping calm

The risk analysis is presented as a formula, because if one item changes, it will affect the level of risk.
- Threats: if the two men who initially pointed at Juan had approached him in a hostile manner, this would still have been less of a threat than a hostile mob forming, and the risk (of assault or murder) would have been reduced
- Vulnerabilities: if the community had not been hostile, or he was with three colleagues (not alone), or he was on a motorbike (or not on foot), his vulnerability would have been less and the risk would have been reduced
- Capacities: if Juan had left his mobile phone at home, or had no credit on it, his ability to deal with the threats would have been much reduced and the risk would have increased. If he hadn't had each of the three friends and allies, he would clearly have been much more at risk. If he hadn't had a plan he might have panicked and run and the mob might have caught him. If he hadn't kept calm, he could have dropped and broken his mobile phone.

Members of the Bagua community demonstrating to protect the land rights of indigenous communities, Peru

This example is not meant to provide a perfect escape plan form a threatening situation. It is clearly specific to this context and is used here to assist you to identify the various components of the Risk Formula and how they can be used to assess the level of risk.

You will see that vulnerabilities and capacities can be two sides of the same coin. For example, if Juan had not carried his mobile phone, that would have been a vulnerability. Having it would be a capacity.

Comments on this case study and the Risk Formula from HRDs:

Comment: 'Isn't the fact that he was well-known and disliked in the community a threat, not a vulnerability?'
Response: In this example, the community's attitude has been long-term. It is not a recent declaration or indication, so it is a vulnerability. If the week before, a community spokesperson had, for example, said in a radio programme that LGBTI HRDs should be hounded out of town, that would have been a threat. Or a stone thrown through his window that morning, that could have been a security incident (if he didn't know who did it and why) or a threat (if it was accompanied by a homophobic message).

Comment: 'This couldn't work in our community – the police would never come to our aid. And 'Why didn't Juan run, or jump in a taxi? Didn't he bring risk to the shopkeeper?'
Response: Yes, all risk situations have different contexts, different vulnerabilities and capacities. Juan also did have other options, but in his assessment, at that time, he made his choice. The case study isn't meant to be a blueprint for a successful strategy (although it did work in this specific context). It is included to illustrate the components of the Risk Formula.

Comment: As it is a formula, like a mathematical formula, shouldn't there be a final answer? If you have 2 threats, 5 vulnerabilities and 10 capacities, doesn't that mean the risk is 1 (2 x 5 = 10. 10 divided by 10 = 1) and therefore very low?
Response: The risk formula is based on human knowledge and subjective assessment. It could be dangerous to reduce it to numbers in this way. It is meant as a tool, to assist you to identify the components in the risks you face, not to provide a mathematical answer to a human problem.

The key messages are:

a) that risk varies depending on the level of threat, but also the level of our capacities and vulnerabilities;
b) that the risk might be different for different actors in the same situation because of their different vulnerabilities and capacities;
c) that even when we cannot reduce the threat we can reduce the risk by reducing vulnerabilities or increasing capacities.

Working with the Police

In some countries, HRDs do not contact the police as a matter of policy, because they believe the police are behind some of the threats they receive. In other countries HRDs work closely with the police. Here are some very different comments from HRDs about working with the police:

"We set an objective to improve our relationship with the police. We worked together with them to set up mobile units to issue driving licences to overcome corruption. This was popular with the police and the community, so we improved our reputation."
HRD, Asia

"An activist was threatened after talking to the UN Special Rapporteur for Human Rights. The police gave him protection." HRD, Asia

"If we talked to the police, someone may see us and say that we are informers. The way we deal with this is to have only formal contacts with high level police officers." HRD, Africa

"We are scared to talk to the police, but we think it is essential to build up our contacts. So in our network of NGOs, we identified one person who already knew the Police Commissioner, who would be the contact person for all our organisations." HRD, Americas

"Some of our members say that the police have carried out atrocities and we should have no contact with them. But our leadership says that if Nelson Mandela could work to develop relations with his captors, we can work with the police in the interests of our country." HRD, Europe

"We know the police support the people who threaten us, but some police officers are our brothers, our cousins and former school friends. They warn us when there is going to be a raid or an arrest." HRD, Africa

Sometimes HRDs have comments on this case study – either in terms of the Risk Formula, or in terms of the tactics used by Juan.

Why is the risk formula a useful tool?

- It is versatile and can work in any part of the world*
- It is flexible and can be used in any situation
- It can be used to predict what capacities will be required in the future – in this case you would define the threats and risks as they might be in the future
- The Risk Formula helps to focus on separate elements. In order to reduce risk, one of these three things needs to happen:
    - Threats are reduced (we will look at this in the next Chapter)
    - Vulnerabilities are reduced
    - Capacities are increased

* However, it may not be suited to communities or cultures where there is no familiarity with formulas, eg illiterate communities. See Appendix 3 for an alternative suggestion of how to discuss issues of risk and threat with illiterate communities.

My Assessment of risks, vulnerabilities and capacities

ACTIVITY

Now list each of the risks you face, and consider your vulnerabilities for each one and then the capacities you already have, and the capacities you have or can reasonably acquire.

Fig. 2.1

Risks	Vulnerabilities	Capacities existing	Capacities required

Notes: . . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .

This exercise results in a basic action plan. We will develop this plan through the following exercise and chapters.

Example: Here is a short example from Matthew, a HRD in Africa. (Fig. 2.2)

Risks	Vulnerabilities	Capacities existing	Capacities required
Abduction	Live alone	Good security at home fence, alarm, camera	Get a guard dog
		Neighbours will keep a lookout for suspicious characters and events	For now, leave a schedule of all my movements with a colleague. If the situation worsens, my cousin should come and stay with me and travel with me
		Other places to stay in times of danger	Communicate with colleague twice a day to confirm I'm safe
Arrest	False charges may be used	Knowledge of the law	
		Lawyer* briefed and ready to act	Learn lawyer's number in case mobile phone taken
		Office and home have no compromising materials	
	Medical condition	Medication	Carry medication at all times

(*Note: in some countries legal process is not followed. In Chapter 5 we look at the plan of a HRD vulnerable to arrest in such a country)

You will see that it is important that you **initially** consider vulnerabilities and capacities in relation to each risk. Knowledge of the law is unlikely to be of any use if you are abducted outside of the law; good neighbours will not be of any help if you are arrested at your workplace.

Many of the vulnerabilities and capacities are common to different risks, so take a few minutes to review your list and group together the risks where the vulnerabilities are similar.

(However, it is also important that you consider other vulnerabilities you have or become aware of. You can never know in advance the totality of the risks you face, so reducing your vulnerabilities overall will give you a stronger base against any type of threat.)

Anara Ibrayeva, HRD and lawyer training HRDs in Kazakhstan on legal issues

Grouping risks, vulnerabilities and capacities

ACTIVITY

Fig. 2.3

Group of Risks	Risks	Vulnerabilities	Capacities existing	Capacities required
Group 1				
Group 2				
Group 3				

Example: This example is to illustrate that some vulnerabilities (and capacities) are common to different risks.

Fig. 2.4

Group of Risks	Risks	Vulnerabilities	Capacities existing	Capacities required
Group 1	Abduction	Live alone		
	Assault	Travel alone	Own vehicle	Plan to change routes, vehicles and time of travel to and from work
Group 2	Arrest		Lawyer* briefed and ready to act	
	Stigmatisation		Legal knowledge	More specialist knowledge about libel and slander
			Office and home have no compromising materials	

More information on some general capacities (the lack of which are vulnerabilities) identified by HRDs are to be found in Appendix 4.

Now you have a broad overview of risks, vulnerabilities and capacities, it is useful to consider how to rank the different threats.

The Risk Matrix - assessing the probability and impact of risks

Sometimes when HRDs live in risky situations for a long time, it is difficult for them to take a step back and assess how risky a situation really is. Also, when the situation for HRDs deteriorates, it is not always clear at which stage HRDs should take action to avoid the danger.

"HRDs living in risky situations for a long time don't always realise when the environment is becoming more dangerous. You can liken the situation to a frog in a cooking pot. If the frog is placed in hot water, it will jump out quickly. If it is placed in warm water on a lit stove, and the water heats slowly, the frog will not realise and will be cooked! We need to constantly assess and reassess the risks."
HRD, Americas

A tool that assists in both of these situations is the Risk Matrix. It can be used as the next step in building up your security plan. It helps you think through the risks you face so you don't spend time considering risks that are unlikely to arise, or risks that don't cause much harm.

First, consider each of the risks you have identified earlier in this Chapter, asking two questions:

1) what is the **probability** of this risk occurring?
2) what will be the **impact** on me if this risk happens?

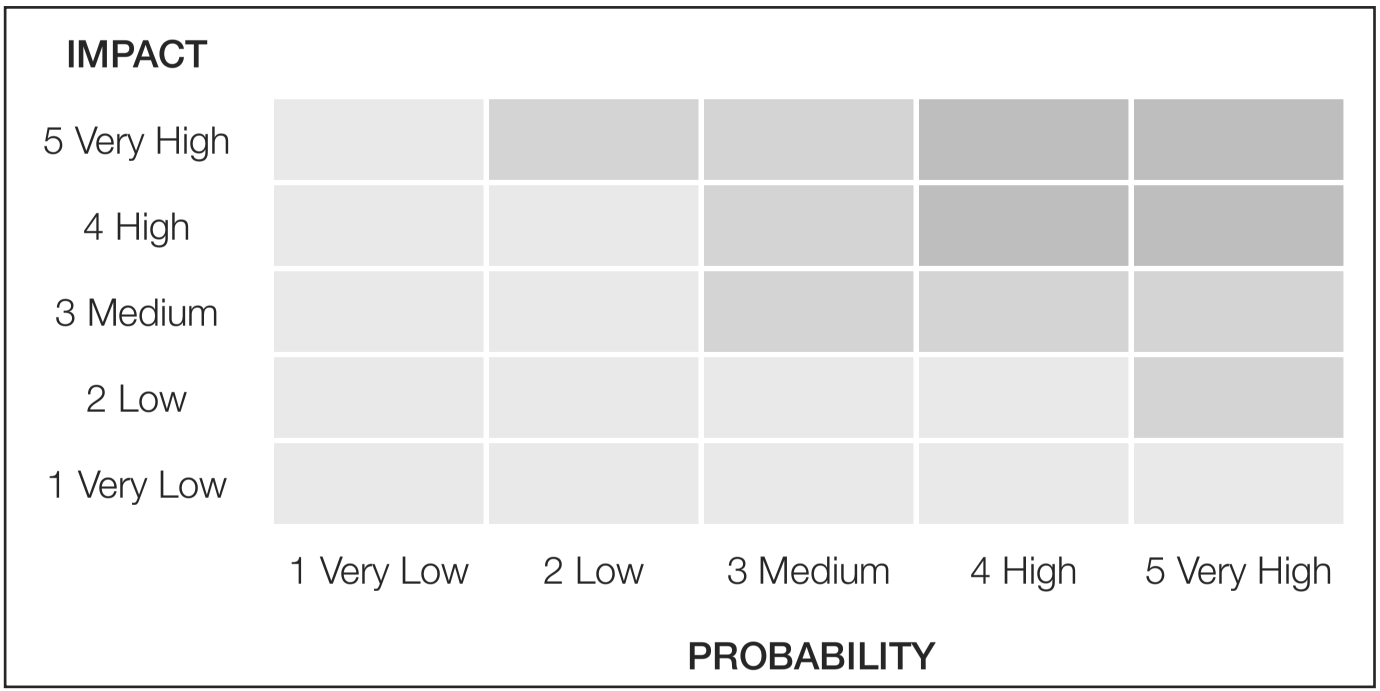
How do you assess probability? This is subjective, but you will base your response on the history of repression and the actions taken against defenders. Similarly your assessment of impact is subjective, but you should take into account the damage to yourself and your organisations, remembering that some HRDs – for example women and LGBTI – are more at risk because they are more vulnerable in some situations.

Father Tomayo, Honduras

ACTIVITY:

My Risk Matrix

Fig. 2.5: On the Risk Matrix below, plot each of your risks in terms of probability and impact. On the following page is an example of how Juan (featured in the story at the beginning of this Chapter) could have plotted his risks.



If the probability of the risk occurring is low, and the impact is low, or the probability is very low (although the impact would be high) - these are the lightest grey cells - you may consider that these are acceptable risks, and use your normal security measures.

For the risks that are probable, but medium to high impact (the medium grey cells in the table), you can produce Action Plans to reduce the probability.

For risks that are high to very high impact (the darkest grey cells), you can produce Action Plans and also a Contingency Plan for each - what to do in case this terrible event does in fact occur in order to reduce the impact.

Juan's Risk Matrix

Fig. 2.6

IMPACT					
5 Very High				Murder	
4 High				Assault	
3 Medium					
2 Low			Robbery		
1 Very Low		Attack on office			
	1 Very Low	2 Low	3 Medium	4 High	5 Very High
			PROBABILITY		

Attack on office – the organisation is very unpopular, but the office is near the police station, so an attack is unlikely
Robbery – this is common in the area. Everyone takes precautions not to carry expensive or sensitive equipment, information or personal resources.
Assault and murder – the probability of these risks rose from medium to high when a high profile colleague was murdered.

Majda Puaca (right) was one of a group of lesbian and gay people attacked during a Queer Belgrade event. She took a case against the leaders of the gang

Assessing risk, impact and probability are key activities in improving your security. However, the assessment needs to be backed up with action – taking measures to reduce the probability of the risk materialising (here called Action Plans) and plans for what to do if the worst does indeed happen (Contingency Plans). Action Plans and Contingency Plans are covered in Chapter 5. Before we look at completing those, we will focus on the second element of the Risk Formula – Threats.

CHAPTER 3: THREAT ANALYSIS

"We know from our discussions with HRDs that they often ignore threats. They sometimes feel that to pay attention to the threat is to give in to those threatening them, or that denial is the best strategy. But we also know that in many cases of HRDs who have been killed they have received threats in the preceding days that they did not react to."

Andrew Anderson, Deputy Director, Front Line

"After the assassination of our Director, I started receiving threats. My organisation set up a whole team to work on different ways to reduce threats. One team considered how to influence the Chief of Police and the Minister of Security. Another team concentrated on getting support from Embassies - especially those which gave bi-lateral aid to the justice and security systems. A third team looked at increasing protection for me at home and whilst travelling. It was a truly organisational response." **HRD, Asia**

This Chapter defines and gives examples of different kinds of threats and security incidents. It proposes five questions to ask in order to analyse a threat. There is a case study of a HRD at risk for you to consider. Then you can apply the five questions to threats you receive. There is a section about security incidents, and a section on surveillance. The Chapter concludes with some strategies for reducing threats.

Dom-an from the Philippines in a role play on receiving and reacting to a death threat

What are threats?

We have defined a threat as a declaration or indication of an intention to inflict damage, punish or hurt.

A threat may be a direct threat against you, your organisation or your family.

Some examples of direct threats HRDs have received are:
"You will not live to see the New Year"
"Your office will be burned down"
"Your organisation will not be registered (be legal) next year if you continue with this type of work"
"We will kidnap and rape your daughter"
Symbolic threats – such as dead animals nailed to the front door

A threat could also be a **possible threat** – such as when other HRDs working on similar issues are threatened and there is a chance that you may be threatened next.

We will also consider here **security incidents** – events which could indicate or lead to a threat.

Examples of security incidents are:

- you think someone may be watching you or your office
- your home or office or car is broken into
- you receive anonymous phone calls

Why are you being threatened?

A threat almost always has a purpose – to stop you from doing something. HRDs often receive threats when their work is challenging powerful actors. The threat shows that your work is being effective – and the threat is intended to stop you having that impact. The challenge is to achieve that balance of managing the threat as far as possible, whilst continuing to be as effective as possible.

It is useful to consider why you are being threatened but not attacked?

- It may be the perpetrator of the threat does not have the capacity to carry out an attack against you and is hoping the threat will be enough
- It may be that the perpetrator is aware of the political costs of attacking you, and is trying to stop your work whilst avoiding the consequences of being implicated in attacking you

However, the situation can change quickly. A perpetrator without resources may gain resources, and the political situation may change so that the perpetrators are willing to risk the consequences of attacking you. **So all threats must be taken seriously and steps must be taken to avoid the risk.**

"When I had completed my research, I wrote a controversial report. I was proud to write my name as the author, but later I realised that identifying myself in that way put me at risk"
HRD, Eastern Europe

"I was invited to be interviewed on TV. I didn't ask the journalist what questions she would ask me. In the event, my interview followed that of the Minister, and I was filmed saying some very negative things about him. After that, a suspicious car parked outside my house for weeks."
HRD, Eastern Europe

"I was assisting a woman who had been raped by two soldiers. The soldiers were arrested and awaiting trial. I began to receive to receive threatening text messages, saying that my family would be burned alive and the family name would be obliterated. After an investigation, it was found that the text messages had been sent by the wives of the two soldiers awaiting trial, who were afraid of losing their husbands and their economic support. I realised they did not have the capacity to carry out their threats."
HRD, Africa

Responses to receiving a threat

Receiving a threat is a shocking experience. Different people respond in different ways.

HRDs who have received threats describe their reactions, and illustrate different types of responses:
"I was petrified! I just stayed at home thinking about the threat and didn't talk to anyone." (paralysed by the threat)
"So maybe they would come for me? I didn't think I could do anything to stop them. I just carried on as normal." (ignoring the threat)
"I started drinking more alcohol." (numbing oneself to the threat)
"My colleagues and I sat down and discussed the threat and what I and the organisation should do." (analysing the threat)
"When I received a threatening text message, I immediately bought a new unregistered phone for use with my family and in emergencies." HRD Asia
Analysing a threat is a constructive response which assists you to deal with the situation.

How to analyse a threat

The purpose of analysing the threat is to find out as much information as you can about the threat, and be able to assess – as far as is possible – the likelihood of the threat being put into action.

This analysis is best carried out with trusted colleagues. They may be more objective than you at this time, and they may be able to contribute different interpretations. (However, in the end, you are the person affected and you should not be pushed to act in a way you are not comfortable with.)

Five questions to analyse a threat:
NB Do not expect that you will necessarily have answers to all these questions.

1. **What exactly are the facts surrounding the threat?**
   - Who communicated what, when and how?
   - If it was a phone call, were there background noises?
   - What was the language and tone?
   - Did it follow some (new?) activity of yours?

2. **Has there been a pattern of threats over time?**
   Patterns could include the following:
   - You receive a series of threatening calls or messages
   - You have been followed for two days and your son was followed yesterday
   - Another HRD was called for questioning by the authorities and then s/he was detained. Now you have been called for questioning

   There could be patterns involving:
   - The type of threats issued
   - The means by which the threat is made (in person, by phone, etc)
   - The timing of the threats (day of the week and time)
   - The perpetrators of the threats (if they are known)
   - The place the threats are made
   - The events preceding the threats, such as your organisation issuing a press release

NB: When the pattern of threats increases in severity, it is an indication that the situation is increasingly dangerous.

Rene Gradis, environment activist in Honduras, has survived two assassination attempts

3. What seems to be the objective of the threat?

Is it clear from the threat what the perpetrator wants you to do? If this is not clear, sometimes the objective can be deduced from the timing of the threat - what actions are you planning or have you have taken recently?

4. Do you know who is making the threat?

- Often you do not know. Do not jump to conclusions
- Be as specific as possible. If, for example, it is a police officer, which station is s/he from? What rank is s/he?
- Consider if a signed threat is really from the person/organisation whose name is used
- If you know who is making the threat, consider if the perpetrator has the resources to carry out the threat. If they have, that increases the likelihood that the perpetrator will follow up on the threat with an attack.

"The President of our country said 'all these HRDs are terrorists'. This increased the number and type of perpetrators willing to attack us. We had to react to this threat at the highest level".
HRD, Americas

5. Finally, after analysing the above questions, do you think that the threat will be put into action?

- This is a difficult assessment to make and you can never be 100% sure
- Your response will take into account your context including the history of attacks against HRDs in your country, the perpetrators' capacities, and the degree of impunity for perpetrators
- When in doubt, choose the option which seems to you to be the safest.

Should you report the threat to the police? Here are some very different assessments from different HRDs:

"Yes, a threat is a crime and the police are responsible for upholding the law."
HRD, Europe

"No, the last HRD who reported a threat to the police was sent back to his family in a coffin."
HRD Middle East

"We work to ensure that laws are implemented in our country – if the local police do nothing we take it higher."
HRD Africa

"Yes, if you can prove you have taken all the usual steps to report a crime but the police do nothing to protect you, you can use this as evidence if you want to use international mechanisms."
HRD, Americas

Clearly you must take your own context into account.

"Although the police can be the ones who attack us, we realised it was essential for us to build relationships with the police at high levels. We held discussions with the Chief of Police to make him aware of the political costs of their attacks on HRDs being publicised. Then one of our members was abducted by two policemen and thrown into the boot of their car. The police hadn't searched him thoroughly and he still had his mobile phone. He managed to phone us and tell us the name of one of the policemen. We immediately phoned the Chief of Police with this information and he called the policemen, who let our colleague go. If we hadn't developed this contact, our colleague would have disappeared for good."
HRD, Africa

Activity – case study

Look at this case study, consider the 5 questions, and compare your answers with the ones that HRDs have provided.

Case study

A woman HRD was sent by her organisation to assist a rural community to protest against the building of a dam which would lead to the displacement of thousands of people and the destruction of a unique ecosystem. The community was virtually united against the construction, although there was a small group who were in favour of the dam because it would bring construction jobs in the short term.

One day, a police officer stopped her husband and said 'you should keep better control over your wife'.

A week later, a message was pinned to the door of their house saying 'Stop causing trouble – or else!'

Three days later, after a lunchtime demonstration, the WHRD returned home to find the house had been broken into, the children's dog had been killed, and a message had been left saying 'You will be next!'.

Consider the five questions, and make an assessment about whether you think the threat to kill the WHRD should be taken seriously.

1. What exactly are the facts surrounding the threat?

.....

2. Has there been a pattern of threats over time?

.....

3. What seems to be the objective of the threat?

.....

4. Do you know who is making the threat?

.....

5. Finally, after analysing the above questions, do you think that the threat will be put into action?

.....

What do you think the WHRD should do? Consider her vulnerabilities and capacities and then her options.

.....

.....

Here are comments by HRDs on this case:

- The context is very important and the facts need to be considered within that context.
- There is a pattern of threats. The police officer warning the husband might not be part of that pattern – it is a security incident where it is unclear if the police officer is speaking as an individual from a patriarchal viewpoint, or if he is issuing the first threat.
- The objective seems to be to stop the WHRD helping the community to mobilise. As the strongest threat was issued during or after the demonstration, it shows that the perpetrators are worried that her efforts may undermine their interests.
- The actual perpetrators are not clear, but the dam project must involve the state (and therefore could involve state agents, such as the police). Foreign governments or companies, who may or may not be sensitive to human rights, are likely partners. Huge amounts of money are involved - therefore the interests being challenged are powerful and influential. On the other hand, the small group in the community in favour of the dam could possibly be the perpetrators – who may or may not be acting in an alliance with the dam project partners.
- The three biggest indicators that this threat can be put into action are:
    - Powerful actors with the capacity to carry out the threat are probably the perpetrators
    - Increasing severity of the patterns of the threats (breaking into the house and killing the dog indicates a capacity for violence and a lack of fear of being caught)
    - Seemingly there is a climate of impunity as the perpetrators feel secure enough to break into the WHRD's house during daylight.

Do you think the threat can be realised? Yes, probably. This is a dangerous situation for the above reasons.

- The WHRD's vulnerabilities include:
    - She is in a new community where she may not have access to or know the normal channels of influence
    - She has her family with her – they may also be at risk

- The WHRD's capacities include:
    - The community
    - Her organisation (although it could be argued that they may also be a vulnerability if they sent her to a dangerous location without a security plan or sufficient resources)

Environmental protection group in La Unión, province of Olancho. When the young people started documenting illegal logging the death threats began. Other members of the community then rallied round to protect them

What should the WHRD do?

There is no 'correct' answer, partly because it depends on the context and partly because there will always be unknowable elements. However, here are some options – some are alternatives, some can be carried out simultaneously:

- Discuss what the WHRD and her family want to do
- Immediately contact her organisation and ask for advice and backup resources – people and/or equipment – and agree an exit strategy in case she has to leave quickly
- Discuss with the community how they can protect her personally, her family and their home – maybe by a system of accompaniment
- Discuss how the community can gather intelligence about the perpetrators of the threat
- Consider what psychological support the WHRD would like at this stressful time

Depending on the results of these discussions, the WHRD could consider these options:

- Leave the area immediately with her family
- Move her family away while she stays
- Increase her physical security by securing the home better (get a guard?)
- Ensure she does not go out alone or leave the family alone, and that a member of her organisation is aware of her schedule and movements at all times
- Consider her local travel arrangements – she may be most vulnerable then
- Report the threats to the police (even though they may be implicated, she will be showing that they have a duty of care and will be documenting the threats)
- Ask for police or state protection (if it is assessed that they are not the perpetrators)
- Call a press conference and publicise the threats
- Network with other local or regional human rights organisations
- Communicate with international organisations who can publicise the case (especially if foreign governments who have a reputation for espousing human rights are involved in the dam project)
- Consider if the tactics of the protest against the dam, and the messages used are the most effective. Depending on the context, she could consider whether asking for a meeting with the dam construction partners in which the community's concerns can be negotiated would be useful.

My threat analysis

ACTIVITY

Have you received threats? If yes, take some time to go through the 5 steps of analysing a threat.

1. What exactly are the facts surrounding the threat?

.....

.....

2. Has there been a pattern of threats over time?

.....

.....

3. What seems to be the objective of the threat?

.....

.....

4. Do you know who is making the threat?

.....

.....

5. Finally, after analysing the above questions, do you think that the threat will be put into action?

.....

.....

.....

Given your own vulnerabilities and capacities, what actions will you take?

.....

.....

.....

Security incidents

We have defined security incidents as events which could indicate or lead to threats. Some examples were given at the beginning of this Chapter. Two more are:

- You have reason to think your emails may be being intercepted
- Unknown people are asking your neighbours or colleagues questions about you

Security incidents may be extremely important indicators of when the threat against you may be increasing, and should never be neglected.

What to do if you experience security incidents

1. Immediately write down the facts and circumstances of the security incident
2. Discuss the security incident with your colleagues
3. Analyse the security incident and decide what action to take

What to do if you experience many security incidents

In some countries, HRDs experience a series of threats and also security incidents. The same principles apply. They should all be written down with as many facts as possible – specific wording, description of personnel, car number plates etc. If you are in this situation, it is a good idea to create a security incident book, where each threat or security incident is logged. Then you can more easily identify if there is an escalation.

If you are working in an organisation, you should make clear that all staff should log any security incidents in the security incidents book. So if, for example, one staff member thinks they may have been followed home, another has their laptop stolen and a third hears that suspicious characters have visited their home, all these are reported and logged. If only one of these incidents happens, perhaps it is just the person's imagination that it is linked to their work as a HRD. But if all these incidents happen within a short period, then it would be a clear indication that negative interest in the organisation is rising and security plans should be moved to a more rigorous level.

"We noticed taxis started parking outside our office. Staff would often take these taxis rather than going to the nearest taxi rank as usual. The taxi drivers started conversations with the passengers, asking what they had been doing that day.

Our organisation regularly met with other organisations to discuss their work and security issues. At the next meeting, we mentioned this security incident. Members of the other organisations present then realised that taxis had also started parking outside their offices too.

We concluded that the authorities were either using taxi drivers to collect information on us, or had planted security personnel as taxi drivers.

Our organisations then decided that the safest response would be to pretend we had not noticed, but we warned the staff not to say anything about their work in the taxis but instead to chat about harmless issues." HRD, Americas

Surveillance

A pattern of security incidents probably mean that you are under surveillance by the authorities or others (although an extremely professional surveillance team may be able to do this work without you being aware of it).

There are three possible reasons why the perpetrators put you under surveillance:

- Information gathering (this may be because of your activities, or because you are

linked to a person or group whose activities threaten the perpetrators)
- Intimidation
- Preparation to detain, abduct or attack you

The reason could change, depending on what the perpetrators believe they find out, or because of changes in the political context.

If you are under surveillance, you and your colleagues need to assess from your experience and from the history of incidents the most likely reason for it. It is important to maintain a balance between taking precautions and not becoming paranoid.
Whether or not you are under surveillance, as a HRD at risk, it is good to develop situation awareness skills. As a minimum:

- Be aware of your instincts – if you think something is wrong, you may have noticed something subliminally – take action to get out of the situation
- Be particularly aware of the possibility of surveillance outside your home and outside your office – a surveillance team will have a 'starting point' where they can be sure of finding you, and generally it will be one of these two
    - Notice anything out of the ordinary – strange characters, unusual behaviour, unexpected gifts (it is best to refuse these – they could be bugged)
    - Notice people you see and describe them in terms of someone they resemble – this will help if the same people turn up in different situations
    - Notice vehicles you see and make a point of remembering key features, eg vehicle make, colour, number plates

In terms of surveillance, it is advisable to:

- Make a plan for how you would deal with this **before** it happens to you – you can agree code words and phrases, or passwords for encrypted messages with your family and colleagues in advance, obtain an emergency phone not connected to your name and arrange access to a vehicle not associated with you for use in emergencies
- Assess the purpose of the surveillance – information gathering? Intimidation? Preparation to detain you? (If you believe you are in danger, take steps to get out of the situation and to a place of safety)

"Communications of HRDs are routinely monitored", Human Rights lawyer Martin Oloo, Kenya

My plan to deal with surveillance

ACTIVITY

If you think you are or could become under surveillance, make a list of the actions you will take to deal with the situation:

- If in doubt, assume that you **are** under surveillance (your person, your phones, your vehicle)
- Avoid putting others at risk
- Act naturally – to check for surveillance you could look outside your house in the morning by taking the rubbish out, or have someone in your home discreetely watch what happens after you leave for work
- Change all your routines: differ the times (and even days) you go in to work, take different routes if possible, do not develop predictable habits (such as always going to the shop or gym or bar at a certain day and time)

"Before we knew how risky it was, we used to challenge the surveillance guys all the time! I would go and take pictures of their number plates and faces with my mobile phone. Now I pretend I haven't seen them."
HRD, Africa

It is generally not advisable to:

- Challenge anyone you think is keeping you under surveillance (this may mean that they will make the surveillance more discreet in future and you won't know it's there)
- Use old-fashioned counter-surveillance techniques such as looking in shop windows (your body language could reveal what you are really doing) or speeding away from a car (you don't know how many vehicles are in the team following you).

For more information, see Appendix 14 on Surveillance Technology & Methodology.

Women Journalists Without Chains in Yemen received a grant from Front Line to install an office alarm system

Note: Remember all the pages on which you can start building up your security plan can be torn out of this Workbook and kept together in a secure place.

"Symbolic actions can help you and your organisation respond to threats and attacks. After our office was ransacked we cleaned the office and then held a symbolic event - coming together with flowers and hope to re-dedicate our office to our struggle for human rights."
HRD, Americas

Khalid El Jamai is one of the few journalists in Morocco who, because of his outstanding reputation, could write an open letter to the King on the issue of torture without suffering severe consequences

Threat Reduction

As mentioned earlier, reducing threats is the most difficult aspect of using the Risk Formula. Reducing your vulnerabilities and increasing your capacities are easier because they are under your control (see Appendix 4: Capacities identified by HRDs).

However, there are some ways you may be able to reduce threats. You can use more than one strategy at the same time. You will have to judge which would work best for you:

- Face the threat:
  - Develop a dialogue with the perpetrators (maybe they do not clearly understand what you do or are not aware your work is legal)
  - Find ways to communicate to the perpetrators the high political cost of threatening or attacking you either directly or via others (eg demonstrate you have influential allies at home or abroad)
  - Publicise the threats you receive

NB: only use this strategy if you think it is safe to do so. Avoid it if you assess it could inflame the situation.

- Share the threat
  - Publish controversial information as a coalition instead of just your organisation
  - Do not put the names of individuals on sensitive reports etc – just the name of the organisation
- Avoid the threat
  - Temporarily stop doing the work that is receiving negative attention (or pretend to stop doing it)
  - Move away temporarily to a safer place
  - Increase your protection measures in other ways, eg:
    - Have people accompanying you at all times
    - Change your routes and routines
    - Be very wary of any new contacts you have not initiated
    - Leave a detailed schedule of your movements with a trusted security contact, who should check in with you regularly during the day
    - Do not deviate from your schedule without informing your security contact

"After receiving threats from conservative religious groups, we approached a leader of one of the biggest Muslim organisations. He agreed to talk at a public meeting and there he said that he supported our work. This reduced the threats."
HRD, Asia

"We use recording devices a lot. We videotape any interviews we give, so we cannot be accused of saying something we didn't. When our office was searched, we filmed the whole event so nothing could be planted. We have a recording device linked to the telephone so we can record any threats we receive. This helps protect us."
HRD, Eastern Europe

Finally, it is important to stress that you cannot foresee the future or know the minds of others accurately, so it is always best to take the approach which seems to you to be the safest.

"I was receiving threats and feeling very vulnerable. The Council of Europe invited me to every Council of Europe meeting that year. I became very well-known and untouchable!"
HRD, Eastern Europe

EU High Representative Catherine Ashton greets Dr Soraya Sobhrang, winner of the Front Line 2010 Award

CHAPTER 4: WELLBEING AND STRESS

In this Chapter we look at what stress is. We then consider the relationship between stress and security for HRDs. We list some ideas HRDs have shared for dealing with stress, and we conclude with space for you to develop your own plan for dealing with stress.

What is stress?

Stress is a totally natural reaction – it is the way our bodies respond to challenges in our environment. Physically, some of the following things happen: our heart beats faster, our blood pressure rises, our mouths go dry and we start to sweat – we are now prepared physically to freeze, fight or flee. Normally this doesn't last very long and generally our bodies quickly return to normal.

Having a certain amount of stress is positive. It can improve our motivation and effectiveness. However, stress can lead to problems when it is intense, and long-term. For HRDs, who may experience prolonged periods of stress, dealing with stress can be a particular challenge.

There is no one solution for stress, because:

- Stress is person specific – what stresses one person may not stress another person in a similar situation.
- Stress is time specific – what may stress one person at one point in time may not stress them at another time, sometimes because their experience mitigates it or the stress has become cumulative.
- Stress is context specific – having similar experiences in different contexts, such as one where you have supportive relationships, can fundamentally change the experience of stress.

Some of the symptoms of stress can be:

Fig: 4.1

On your body	On your mood	On your behaviour
Headaches	Anxiety	Angry outbursts
Muscle tension	Anger	Irritation
Change in sleep patterns	Depression	Eating more or less
Exhaustion	Paranoia	Drinking more alcohol
Change in sex drive	Jealousy	Smoking more
Digestion problems	Restlessness	Social withdrawal
Feeling dizzy	Mood swings	

Stress, HRDs and security

The life of a Human Rights Defender (HRD) at risk can be inherently stressful.

This stress may be the result of human rights violations you experience personally, threats received, the risks you face because of your work, witnessing atrocities, assisting people who are traumatised, dealing with the seemingly never-ending demands of work, and the difficulties of balancing work and relationship/family responsibilities.
HRDs have identified the management of stress as one of the factors impacting their security. Those who have been through periods of deep stress have explained different security-related aspects, such as:

- becoming careless of danger
- finding it difficult to take decisions

- physical exhaustion
- alienating sources of support through angry or moody behaviour
- drinking more alcohol
- feeling 'burnt out'

Tools for Wellbeing

Stress will affect you less if you take good care of yourself daily in these 4 basic areas:

Relaxing after a workshop

Diet – sit down and eat balanced meals with lots of fruit and vegetables. Avoid fast food. Limit stimulants such as coffee, alcohol and sugary foods and drinks, which can cause emotional highs and lows as well as other health problems.

Exercise – stress produces chemicals in the body to prepare us for fight or flight. Fight or flight may have been the best strategies when humankind hunted wild animals to survive, but for most of us, times have changed! Exercise is a healthy way to reduce these stress chemicals. Aim for 30 minutes of activity, such as walking, each day. Three to 4 times a week, aim to do exercise which raises your heartbeat, such as playing football, dancing, running etc, for 20-30 minutes. Build this up slowly if you haven't been very active recently and check with a health professional first. Exercise usually has instantaneous effects on your sense of wellbeing, as well as wide-ranging health benefits.

Relaxation – spend some time every day relaxing your body and mind. This could be yoga, praying or meditating or just taking a few deep breaths. Build relaxing activities into your week.

Sleep – (each person is different but all need between 6 and 8 hours) – but if you look after yourself in terms of diet, exercise and relaxation, then generally sleep should not be a problem.

Organisations where HRDs work should consider how they can improve the stress levels of their staff, for example by:

- making it clear that talking openly about risk is encouraged
- encouraging people to take breaks/holidays and discouraging a culture of regular excessive working hours being a badge of dedication (exhausted people working long hours generally results in a decline in work quality)
- organising practical and/or symbolic activities which encourage and strengthen the team spirit

"Sometimes the incidences of human rights violations seem relentless. In our organisation it is important to celebrate our small achievements - such as a successful resolution of one client's case. This helps us remain positive. We know that we cannot individually move a mountain, but if each person takes one stone, eventually we can dismantle it."
HRD, Middle East

HRD sharing their ideas for dealing with stress

Everyone naturally enjoys activities which relax and absorb them. These stress-reducing activities were shared by HRDs from Africa, Asia, the Americas, Europe and the Middle East:

- Writing (I sometimes do automatic writing – that is, writing without thinking what is coming out of the pen)
- Going to my religious centre to pray
- Going for long walks
- Meditating
- Playing football
- Talking to a therapist or my sister

"Front Line is developing a stress management programme and each week we have a session where we test and practice the techniques we have learned. There's something that suits everyone. We also have regular social events - football matches, film shows, parties and other celebrations."
Mary Lawlor, Director, Front Line

- Writing articles on issues that I feel helpless about
- Playing with my children
- Dancing in my community
- Spending romantic time with my partner
- Going for a run
- Having a massage
- Sitting down quietly with a cup of tea
- Writing to my networks for support
- Letting myself sleep for as long as I want
- Going to the gym
- Listening to music
- Turning off the phone for few hours
- Giving myself a treat
- Having a long bath

Activity for your Plan:
Now produce an action plan to deal with your stress.

Consider what you already do to reduce your stress:

. . . . . .
. . . . . .
. . . . . .
. . . . . .

Can you do that activity more frequently?

What other techniques have you always wanted to make time for or try? Look at the list created by other HRDs in the previous section – would any of those techniques work for you? Write a list of commitments you make to yourself to reduce stress and a concrete plan for how you will incorporate more stress-relieving activities into your life.

Bernadette Ntumba, Eastern DRC - a symbolic action with stones and flowers commemorating the lives of WHRDs

My plan for improving wellbeing

ACTIVITY

Fig. 4.2

	Improvement	Timing
Diet		
Exercise		
Relaxation		
Other		

Here is an example from a HRD:

Fig 4.3

	Improvement	Timing
Diet	Have a sit-down breakfast	Every morning
Exercise	Go for a walk Play football with friends	Mon, Wed, Fri Sat
Relaxation	Play with my children (more) Take holidays	At least an hour a day 3 times a year
Other	Stop taking work home Discuss the reasons for my stress with my wife and brother Go to bed before midnight, Mon – Fri	

There are many tools available to help lessen stress. The most important tool at your disposal is your own mind. When you recognise for yourself that you experience negative stress, then is the time to decide to do something about it.

Reducing your stress is a process which requires some time investment from you, but will reward you richly by making you happier, more resilient and more effective in your relationships and work. A less stressed HRD is undoubtedly a more effective HRD.

The contents of this section of the Front Line Workbook are not meant to replace therapy or other professional help where that is necessary and available.

Standing in solidarity. Members of The Borok People's Human Rights Organisation, Tripura, India

CHAPTER 5: CREATING SECURITY PLANS

> ***" I thought that making a security plan would be a big undertaking. Yes, it can be big, but some of it you can develop as you learn. It need not be complicated."***
> **HRD, Middle East**
>
> ***"I travelled from South Africa to run a workshop for Human Rights Defenders in Liberia when we thought the war was over. One night we heard machine gun fire and mortars in the nearest village. I had no plan for what to do. Now I know better..."***
> **HRD, Africa**
>
> ***"Putting together and implementing a security plan saved my life."***
> **HRD, Americas**

In this Chapter we will look at three different strategies for considering security: the acceptance strategy, the protection strategy and the deterrence strategy. We will then look at how to create security plans - for yourself and for your organisation.

Introduction:

This is the final phase of this Workbook. Now you can bring together the learning from the previous tools you have used – Context Analysis, the Risk Formula, the Risk Matrix, questions for threat analysis, and your plans for dealing with stress.

Three security strategies

First, we will look at **three types of approaches to security**. You and / or your organisation may naturally or deliberately have a policy or preference for one type of strategy, but it is useful to look at all three and consider their attributes.

Acceptance strategy: an approach which involves negotiating with all actors – the local community, the authorities etc, to gain acceptance and ultimately support for the organisation's presence and work. Although this requires careful planning and can be labour-intensive, it may be the most effective strategy in the longer term to reduce threats. This approach usually entails high visibility, so in times of great threat it is sometimes more difficult to adapt to being more low profile.

"Making ourselves more visible can be one of the best protection activities. When we meet leaders of regional or international organisations, we insist on having our photo taken with them. We display these photos at our office for everyone to see."
HRD, Asia

"I go fishing with an old school friend, who now works in a government ministry. He tells me a lot of useful information in this relaxing environment."
HRD, Eastern Europe

Protection strategy: an approach which emphasises security procedures and protective elements. Impact is mainly on reducing vulnerabilities. Can of course be used in conjunction with the other two strategies to strengthen protection.

Deterrence strategy: an approach which relies on counter-threats for protection. For example, if threatened, an organisation might react by taking a legal case out against the person issuing the threat, or by publicising the threat, or responding to the perpetrator by explaining the consequences of carrying out the threat – such as international condemnation. This approach should only be used if you have accurate information and powerful allies.

When you are developing your security plans, consider how elements of acceptance, protection and deterrence can expand the menu of options you have at your disposal.

UN Special Rapporteur on HRDs Margaret Sekaggya with Abdulhadi Al Khawaja – currently in prison in Bahrain

Production of Security Plans

We are now going to consider how to produce Security Plans. In human rights organisations where the HRDs are at risk, an organisational security plan will help to protect the workers and allow them to do their work more effectively. If your organisation acknowledges and plans for dealing with the risks, the staff and/or members will feel more supported and have increased allegiance to the organisation and its important work.

We will start however, by considering a Security Plan for an individual. This is for a HRD working on their own. A HRD working in a human rights organisation might also find it useful to have their own individual security plan but generally it will be more effective, for the individual and the organisation, to have an organisational security plan discussed and agreed collectively. Although each individual has unique attributes (such as gender, sexual orientation, age, experience, position in organisation, location of home etc) which make them more or less at risk, individuals will generally make better security plans when drawing on the different experience and perspectives of different members of the group.

Also, where there is an organisational commitment and culture of security the individual is more likely to adhere to agreed security measures. The risk of individual security plans is that they become personal good intentions that get thrown out when things are hectic.

There is also a risk in many organisations that the more high profile and experienced HRDs take all the responsibility for security planning and management in a way which does not build the capacity of other members of the group and can leave the organisation paralysed if the experienced leader is removed. However, an Organisational Security Plan may not cover at all, or may not cover fully, reducing risks in your personal life so it can be helpful to develop a Personal Security Plan as well. And developing a Personal Security Plan can also be good preparation for a discussion on an Organisational Security Plan.

A WHRD, for example, whose husband feels threatened by her high profile and is becoming violent towards her, will have to consider in her Personal Security Plan how to deal with the increasing threat from within the home.

Then we will look at the process for producing an Organisational Security Plan and its contents.

If your organisation does not have an effective Security Plan, you can use this Workbook to assist your organisation to develop one. If your organisation is resistant to creating an Organisational Security Plan or it has a plan but it is not effective, see Appendix 15, *Overcoming Resistance to Security Planning*.

1. Producing a Personal Security Plan

Reminder: Did you identify factors, as suggested in Chapter 1 of what makes you feel secure and what makes you feel insecure? If yes, review this now. Some of the items you identified may become part of your plan. You should by now have more items to add to increase your feeling of security.

Your Personal Security Plan can comprise security policies and procedures and contingency plans You can begin your Personal Security Plan by focusing on two or three risks you face (which you wrote down on Fig 3.1 and perhaps also Fig 3.2). Perhaps you face more than three risks, in which case you can return to include the others later, but focusing on two or three to begin with makes the process easier to manage. Most HRDs choose to focus on two or three risks which are medium to very high impact, and medium to very high probability (see Chapter 2).

If you have not already done so, plot each of the risks on the Risk Matrix (Fig 3.5) by assessing how likely they are to happen (their probability) and what impact they will have on you if they do in fact occur. To do this you will use your experience and knowledge of the political situation. It is a subjective assessment.

HRDs at the Dublin Platform networking with Navi Pillay, UN High Commissioner for Human Rights

For the risks you have identified as moderate to very likely probability, you can draw up an Action Plan. This aim of this is to reduce the likelihood of the situation occurring.

Opposite is a very simple example - it is not meant to be a blueprint for your situation. You can look at more examples of points to consider including in the Appendices. However, you are the person best placed to know what will be most effective, given your unique situation of capacities and vulnerabilities.

My Personal Security Plan

ACTIVITY

Risks:

Risk 1 . . . . . .

Probability . . . . . Impact . . . . . .

Threat assessment: . . . . . .

Vulnerabilities: . . . . . .

Capacities: . . . . . .

Action Plan:

1. . . . . .

2. . . . . .

3. . . . . .

4. . . . . .

5. . . . . .

Risk 2 . . . . . .

Probability . . . . . Impact . . . . . .

Threat assessment: . . . . . .

Vulnerabilities: . . . . . .

Capacities: . . . . . .

Action Plan:

1. . . . . .

2. . . . . .

3. . . . . .

4. . . . . .

5. . . . . .

ACTIVITY CONTINUED:

My Personal Security Plan

Risks:

Risk 3 . . . . . .

Probability . . . . . Impact . . . . . .

Threat assessment: . . . . . .

Vulnerabilities: . . . . . .

Capacities: . . . . . .

Action Plan:

1. . . . . .

2. . . . . .

3. . . . . .

4. . . . . .

5. . . . . .

Example only:

Personal Security Plan

Risk = Arrest in the context of police search of home and confiscation of papers / phone/ laptop
Probability of this happening: medium to high – other HRDs have been targeted in this way recently.
Impact if it happens: medium to high for myself, my family and my organisation
Threat assessment: Police usually raid homes in the early hours of the morning
Vulnerabilities:
- There is no due legal process - there will not be a search warrant or right to have a lawyer present
- We deal with sensitive information in my organisation
- My young children live at home

Capacities:
- Ability to plan (thinking through how you can best respond in advance reduces the losses you could incur)

Action:
1. Discuss the risk with my spouse and tell him who to call if the police arrive. (possibly getting colleagues / friends to witness the search if their presence will not put them at risk of arrest too) and who to call afterwards (eg human rights organisations)
2. Arrange for the children to sleep at their Aunt's at times of heightened risk
3. Investigate possibility of CCTV in home to record event
4. Be aware of my rights in detention so I can request them authoritatively (even though they probably won't be granted)
5. Have a lawyer briefed in case I am allowed access to a lawyer
6. Do not store sensitive work information at home
7. Delete sensitive information from computer and phone
8. Ensure all my personal affairs (taxes etc) are in order so that they cannot become a pretext for a political prosecution)

Next, for any risks you face which have high to very high impact on you, you can draw up an Action Plan and a Contingency Plan. See overleaf for a short example based on the experience of HRDs who have been faced with kidnap by tribal groups.

"The security forces came to arrest me at our office. They wanted to do it quietly. I quickly sent a text message to a whole group of people with a pre-arranged code about an urgent meeting. When 50 people arrived, the security forces left."
HRD, Asia

Personal Security Plan

Risk = Kidnap
Probability of this happening: moderately likely - HRDs who travel in rural areas are sometimes kidnapped by tribal groups. I frequently travel in rural areas for my work.
Impact if it happens: Medium to Very High - some victims of kidnaps have been well-treated; others have been assaulted, raped and killed.
Threat assessment: Perpetrators are from different tribal groups, depending on the area, and are heavily armed
Vulnerabilities:
- I need to travel to areas where kidnaps occur and I could be easily identified as non-local

Capacities:
- Our organisation has funds for security
- Ability to plan for this (thinking through how you can best respond in advance reduces the likelihood)

Action Plan:
1. Consider whether it is safer to travel in a more high profile way – eg publicly, maybe with a high profile person, perhaps in a secure convoy, OR
2. Travel in a low profile way, perhaps on public transport, wearing clothes worn by local people in the area
3. If possible travel with a colleague / companion who will act as some protection, for example because s/he is known in the area / speaks the local language etc
4. Do not travel without having a trusted local contact at my destination
5. Leave schedule of travel plans with designated colleague, and check in with her/him twice a day to confirm all is OK
6. Prepare list of contact details of village elders who have worked with our organisation and could negotiate with the kidnappers – take it with me and also leave a copy with the organisation
7. When travelling, do not follow specific routines
8. In villages, only go where trusted local contact recommends
9. Be aware of what is going on around me at all times (situation awareness) and take action immediately if something does not appear normal.

Contingency Plan:
If I am kidnapped:
1. Stay calm and quiet – especially in the initial process of being kidnapped when the kidnappers will be most nervous and prone to violence
2. Do not try to escape – unless the kidnappers clearly intend the worst
3. Ask to send a message immediately to my organisation
4. Try to gain the kidnappers' respect and build rapport with them
5. Obey orders without appearing servile, but also ask for improved treatment
6. Take care of health: eat and exercise
7. Keep busy by memorising details, descriptions of perpetrators, possible locations, number of days as they pass, etc.
8. Know my organisation has a plan for negotiating for my release and they will do everything in their power to achieve that.

"I was kidnapped by agents of the military. I realised the location I was in because of the address of the shop on the take-away food wrapper. I was blindfolded and questioned. When I was finally released I was later able to identify one of the perpetrators by linking the smell of his aftershave with his voice. Although this information was not enough to charge the perpetrator, consciously collecting this information at the time gave me a sense of control."
HRD, Asia

Note that Appendix 9 also contains a check list on detention / abduction, with some more suggestions.

Security plans are key building blocks for your security situation. But they may not cover every eventuality. Create a habit of considering "what would I do now if (a certain event happens)?" which develops your capacity to react to both the anticipated, but also the unexpected.

Security plans and procedures are valuable tools, but they also have to be balanced by situational awareness, common sense and good judgement.

2. Producing an Organisational Security Plan

First we will look at the process we recommend for producing the Organisational Security Plan, then at the contents.

The legal responsibility for staff may differ from state to state. Be aware what the legal position is in your country and include Board members in your discussions as appropriate.

2.1 Process of producing an Organisational Security Plan

We recommend you allow a day for the initial discussion. For equipment, you will need a flip chart and paper.

2.1.1 Bring together all your trusted colleagues to **discuss and list the risks you face** as an organisation and as people working within the organisation. Including as many staff as possible in this discussion will begin to build security awareness and commitment to adhere to security measures. Support staff such as the receptionist and driver may not be the most at risk, but they may be the first to spot security incidents. Encourage everyone to contribute and consider each contribution seriously.

Aftermath of police raid, Western Sahara

Include also in your discussions the way in which you work with groups and individuals - survivors of violence, witnesses etc – and the risks they may face because of contact with you. (You may decide to have a meeting later with representatives of these groups and individuals to check with them the viability of your security plans as they relate to them.)

2.1.2 Prioritise the risks using the Risk Matrix. For each risk, try to find agreement on how probable the risk is and what its likely impact will be – for the people concerned and for the organisation. Log these on a copy of the Risk Matrix. Most organisations would choose to focus on those risks which are medium to high impact, and medium to high probability. In your discussions participants may also identify easy, low cost options for dealing with lower risks. These suggestions should be accepted and implemented if possible but do not lose sight of the most important risks.

2.1.3 Group the risks. So, for example, if your office is vulnerable to burglary and physical attack of the premises, create a category of 'risks to office security' (but write an explanatory sentence of what it is intended to cover below, so the real risks do not become hidden over time).

CCTV for human rights organisation funded by Front Line

2.1.4 Agree the contents of the security plan – see (2) below for ideas. You will need to include security policies and procedures and contingency plans.

2.1.5 Pick one of the biggest risks. As a large group, **discuss, agree and document what will be in your plan to reduce your vulnerabilities and increase your capacities in relation**

to this risk. If you have time, consider more risks. (You could do this by splitting your group into smaller groups, to save time. Allocate one different risk per group. Ask each group to feed back to the full group to present their plan. Discuss each presentation and agree the final plan for those risks.)

2.1.6 **Allocate responsibility for producing a draft plan for each remaining risk** to those most suitable to draft them. Give a deadline for production. Meet again at that deadline to **discuss and agree the final plans for the remaining risks and the final version of the Organisational Security Plan**.

2.1.7 **Communicate the Organisational Security Plan to those who need to act upon it** – preferably all staff. Although you may circulate the document, it is best to present it face-to-face to allow everyone the chance to discuss the importance of security and the Organisational Security Plan.

2.1.8 Ensure that **one person is responsible for monitoring the implementation and review of the Organisational Security Plan**. It might be better if this is not the leader of the organisation who will have many other concerns.

2.1.9 The Organisational Security Plan is a **work in progress**. It should be adapted any time new tactics for your security arise. It should be reviewed when a new risk arises, or a threat is received, to check that your tactics are adequate to deal with the danger. It should also be reviewed after this new danger dissipates, to check that the Organisational Security Plan made sense in the situation and was followed. When the Organisational Security Plan is revised, the **version and the date should be clearly identified**, so it is clear which is the up-to-date Plan.

2.2 'Traffic Light' Security Settings

Some HRDs advocate also having a simple plan based on traffic lights.

If the situation is 'Green', then all is proceeding as normal and no special security precautions need be taken.

If the situation is 'Amber' then there is increased risk and a number of precautions need to be taken.
If the situation is 'Red' then this is the highest risk situation and the highest security measures need to be taken.

Each organisation would need to create its own Traffic Light Security Settings based on their own context, threats, vulnerabilities and capacities. But here is a short example:

Example: 'Traffic Light' Security Settings

"We talk to our donors in advance about financial assistance to improve our security, for medical and life insurance, and how our families will be supported if we are imprisoned or killed." HRD, Americas

The advantage of the Traffic Light Security Settings is that they are simple. They are easy to communicate to a large number of people and to communicate when the security setting changes. However, they are not a replacement for a fully thought through Organisational Security Plan and the development of awareness of security issues throughout the organisation.

Fig 5.1

Alert Level	Staff	Work Projects	Office
Green	• No restriction	• No restriction	• Normal security
Amber	• Staff most at risk (decided in advance) work at home • No staff to work alone in office or outside designated office hours • Reminder of who to ring in emergency • Alerted trusted neighbours / local community	• Sensitive projects put on hold (decided in advance which are sensitive) • Lawyer alerted • Other work continues	• Guard hired • No visitors allowed • Check no sensitive information available in office or homes • Alert trusted neighbours / local community • Alert police (if appropriate)
Red	• Staff most at risk relocate (which staff and where is decided in advance) • Other staff do not come to work	• All work halted temporarily • Advise donors	• Office locked • Additional guard hired

2.3 Contents of an Organisational Security Plan

Every organisation producing an Organisational Security Plan will do it differently, depending on their context, the risks they face, the threats they receive, their vulnerabilities and their capacities.

Overleaf are some headings which you may wish to consider for inclusion in your Organisational Security Plan.

"All our staff know what a search warrant looks like. They know how to check it. They know if the authorities come to search our office they do not have the power to search the people too. So if our office is to be searched, we hide our small laptops down our jeans."

HRD, Eastern Europe

Fig 5.2

Heading	Examples of Possible Content	Notes
Organisation's mission	Eg "We provide free legal assistance for people who can't afford lawyers"	This should be short and concise; staff should be able to repeat it quickly (eg at a road block)
Organisation's statement on security	• Staff may refuse assignments if they assess them as too dangerous (without disadvantaging themselves)	
General statement on security	• Security is not just about obeying procedures, but about always practising situational awareness and common sense • Security is for everyone – if one person neglects one area, it can put the whole organisation at risk	
Key roles and responsibilities	• Person who is overall responsible for security • Duties of other staff, including planning and evaluation, insurance, implementation. • Individual responsibilities: following rules and procedures; reducing risks, communicating security incidents, safety in personal life	Job titles are better than names – they tend not to change
Crisis Management Plan	• Definitions of types of emergency that brings this Plan into action • Roles and responsibilities, including: setting up a Crisis Committee, communicating with staff, with relatives, with authorities, with the media, with donors, etc.	For unanticipated emergencies
Security Policies and procedures	• Office security • Home security • Dealing with clients, witnesses etc • Computer and phone security • Information management and storage • Going on field trips • Vehicle maintenance and use • Avoiding attack (theft, assault, including sexual assault) • Dealing with cash • Dealing with the media • Dealing with the authorities • Stress reduction in the organisation	The contents will relate to your context. Some of the policies and procedures will overlap; repeating the procedures is better than complicated cross-referencing
Contingency Plans	• Detention / Arrest / abduction / death • Assault, including sexual assault • In the event of a coup	These are 'what to do if...' plans. The ones you need depend on your context and the risks you face.

Documentary made of HRD the Venerable Sovath Luon (right) helped raise profile and provide protection

CHAPTER 6: UNDERSTANDING YOUR CONTEXT

In this Chapter, we will look at some reasons why a context analysis can be useful, with whom and when to do it. We introduce two tools for context analysis – Context Analysis Questions and an Analysis of Actors. There is also a simpler tool in Appendix 1 – SWOT (Strengths, Weaknesses, Opportunities, Threats) Analysis.

Participants at a security training work through an Analysis of Actors

Why is a context analysis useful?

"There are so many armed groups! A HRD working in this area must be able to identify each type of group – their location, appearance, their aims and methods. If you don't and you see armed men, you don't know what your best protection strategy is. If the armed men are robbers, I know they only want to steal the vehicle and they will let me go. If they are narco-traffickers, then they will try to kill me, so I need to accelerate out of there! We developed this knowledge of the aggressors in the area with the local communities – and we make sure all our workers know what to look out for and what is likely to be the best action to take in a dangerous situation" HRD, Americas

"In our country, knowing influential people is the best protection mechanism. We had discussed in our organisation which high level contacts we had connections with. When our female colleague was detained, we knew that her grandfather was a friend of a senior government official, so he was asked to advocate for her release – this was a successful tactic." HRD, Middle East

"So we can be effective in human rights work, we have developed an in-depth knowledge of our context – our history, our political system and our culture. We know who our opponents and supporters are, how they work and what motivates them. And when we discussed these issues, we realised that we had not considered how to transfer this knowledge to the crucial context of our security! We then spent some time considering how these factors related to our security, and fed the results into our security plan." HRD, Europe

HRDs work in extremely complex environments with many actors and interests. HRDs working in the same area for a long time develop deep knowledge about the context of the work.

However, taking some time to re-conceptualise and re-analyse this knowledge in the context of security will benefit your organisation in many ways. You can share new information, such as access to or how to get in touch with influential contacts, and document the resources you have so that others can benefit from your expertise. You can draw new lessons from your environment in terms of security, raise awareness in your organisation about strategic actions and contacts, gain fresh insights and recognise new opportunities.

With whom and when to do a context analysis

The best context analysis is carried out with a group of trusted colleagues. This collaborative sharing and mapping draws out aspects of insecurity and enables less experienced colleagues to better understand and manage their security.

A good time to do this is during the development of your organisation's plan for the next planning period (or when there is a clear change in the security environment in which you work). The process will clearly identify opportunities where you can weave security and protection strategies into your activities. Below we suggest two tools to use for this process, which are ideally used consecutively.

Depending on the size of the organisation, and the level of trust, not every person in the organisation might participate in this discussion, but it is essential to document the key points and clearly communicate to others in the organisation what they need to know.

However, if the paragraphs above don't apply to your situation, perhaps you are a HRD working alone, we suggest that you (with others if at all possible) start with the simpler SWOT (Strengths, Weaknesses, Opportunities, Threats) Analysis on security in Appendix 1.

If you can take the time to put thought, research and analysis into considering your context, the clearer and more focused your protection strategy can be.

Tools for context analysis

1. Context Analysis Questions

Below are some useful questions to answer for a context analysis. (You can find an example of one organisation's answers in Appendix 2: Context Analysis Questions.) The questions are only a guide and you may find that different questions would be more suitable for your unique situation.

Reminder: If you are part of an organisation, you can get the best results if you discuss the question as a group.

Fig. 6.1

Context analysis questions:

1. What are the key issues which impact on human rights in the country? (Consider political, economic and social issues)
2. Who are the main actors on these key issues? (Consider powerful individuals, institutions, local, national, regional and international organisations, business and other states)
3. How might our human rights work negatively or positively affect the interests of these key actors – how have they responded already?
4. When are HRDs most likely to be attacked (verbally or physically)? (Eg prior to or during elections, after publishing reports or naming key figures publicly, demonstrations, anniversaries, high-level visits, events etc)

"We were monitoring and documenting information on killings and other abuses by state forces controlling the diamond field. Our state began to negotiate re-entry to the Kimberly process (which aims to regulate the sale of diamonds so that they are not associated with human rights violations). Our NGO's Director was arrested and charged with 'communicating and publishing falsehoods about the state." HRD, Africa

(The charges were later dropped after months of sustained national and international pressure.)

Clearly the NGO's work deeply challenged key strategic issues of the Government and security forces by calling international attention to human rights violations and thereby threatening economic interests.

Your work may to a greater or lesser extent challenge the key strategic objectives of those in power. If it relates directly to a key strategic interest, you may risk severe repression when your work becomes increasingly likely to have an impact.

It is important, therefore, to have flexible security planning which includes consideration of the safest ways to carry out challenging actions, and leads you to adapt, increase or create new security measures at times when the risk increases.

Our next tool is used to look more specifically at actors, their relationship to your security – and to each other.

"Every week we discuss our forthcoming activities and their implications for our security" HRD, Americas

2. Analysis of Actors

An Analysis of Actors can help you deepen your understanding of those who have a negative or positive interest in and impact on your security. It will help you to identify the interests and conflicts, and lead you to develop insights into potentially productive relationships. It should enhance and expand your knowledge base, and assist you in choosing the most effective actions in relation to your security.

It can take some time to develop (and it will need to be updated either annually or in times of change) but it will be an invaluable resource.

Reminder: There is a simpler tool (a SWOT – Strengths, Weaknesses, Opportunities, Threats - analysis in Appendix 1.)

Reminder: it is best to do this in a group, to share knowledge and experience.

You will need some paper and marker pens. The best way to do this is to cover a large section of your office wall with flip chart paper so you have lots of space.

Step 1) Make a list on flip chart paper of the different stakeholders or actors (state and non-state) with an interest - positive or negative - in the security of you as a HRD or your organisation. (You may have already done this by answering the discussion questions in Fig 6.1 above.) Examples could be: Office of the President; Ministry of the Interior; army; police; armed opposition groups; political parties; religious groups; media; commercial enterprises; international NGOs; national NGOs; foreign embassies; community leaders/elders, relevant communities.

If you are in a rural area, you might decide to concentrate on the area or region, rather than the national level. Ideally you would do both.

Fig. 6.2 Example: Analysis of Actors

	Government	Police	Religious Institutions	Media	International NGOs	Armed Opposition Groups	Army	UN Agencies	National HR NGOs	Other States
Government	X		**SAMPLE 1**							
Police		X								
Religious Institutions	**SAMPLE 2**		X							
Media				**SAMPLE 3**						
International NGOs					X					
Armed Opposition Groups						X				
Army							X			
UN Agencies								X		
National HR NGOs									X	
Other										X

SAMPLE 1: How do religious institutions influence Govt?

SAMPLE 2: How does Govt influence religious institutions?

SAMPLE 3: a) Interest in good topical stories. fear that govt could close them down. b) Coverage of events; printing articles from HRDs; c) Power to protect – high; d) Readiness to protect – medium

Step 2) When you have your overall list, consider which of these should be split down into sub-categories to best reflect the differences within entities or groups. For example, the Ministry of the Interior may be responsible for the police (who are opposed to your work and will not automatically protect you) and also a unit charged with the protection of HRDs (which may be trying to develop a good reputation for protecting HRDs). There are also likely to be differences in the relationships HRDs have with state-owned and private media, with different religious groups, different embassies, diverse communities etc.

Step 3) Next count the number of actors you have identified and draw a grid with that number + 1 of (vertical) columns and the same number of (horizontal) rows as columns.

Leaving the top left-corner box blank, list the actors in the same order both across and down the page.

Step 4) For each box where the actor name is the same vertically and horizontally (see the boxes marked X), fill in:

a) their aims and interests in relation to protection (or attack) of HRDs
b) their strategies for attacking or protecting HRDs
c) the power they have to attack or protect HRDs (you could use: power (protect or attack) - low / medium / high)
d) their readiness to attack or protect HRDs (low / medium / high)

The 'Media' box is shown as an example (see fig. 6.2)

For the other boxes, you will consider the relationships between the stakeholders in terms of protection of HRDs. So starting from the top row, consider the relationships and influences between the top row actor and the other actor intersecting that box.

For example, in the (vertical) column headed Religious Institutions which intersects with the horizontal row entitled Government, consider the way the religious institutions influence the Government. And in the column headed Government which intersects with Religious Institutions, you will consider how the Government influences the religious institutions.

When you have finished the analysis, make a note of implications that have struck you.

. . . . . .

. . . . . .

. . . . . .

. . . . . .

Examples of insights that an Analysis of Actors provokes are:

- we are not yet in contact with some of the actors with power to protect HRDs
- there are some actors who attack HRDs who may be susceptible to influences from actors who have power to protect us (eg the President may be very sensitive to the media)
- some powerful actors who attack us may also have some elements of readiness to engage with us – are we taking opportunities to do so?

"My neighbours denounced me to the authorities as a 'state enemy'. When I helped the community gain more equitable access to electricity, my neighbours started appreciating what human rights really meant, and began to support me." HRD, Eastern Europe

"We assumed the Editor of a conservative newspaper would not be sympathetic to our work. When we had a meeting with him on concrete proposals to assist indigenous people, he agreed to all our proposals! This encounter developed our relationship with him and his newspaper started covering our events more frequently." HRD, Africa

Final comments:

Security plans are essential building blocks in considering your security situation. One of the greatest learning associated with them is the time spent in considering 'what if...?' which develops your reactions to both the anticipated, but also the unexpected.

Security plans and procedures are valuable tools, but they also have to be balanced by situational awareness, common sense and good judgement.

Front Line warmly welcomes any comments on this Workbook. Please send them to: **workbook@frontlinedefenders.org**

Dr Mudawi, Sudan, Inaugural winner of the Front Line Award 2005 with President of Ireland, Mary McAleese

Selected bibliography:

Barry J, Nainar V, *Women Human Rights Defenders' Security Strategies: Insiste, Persiste, Resiste, Existe*, Urgent Action Fund, Kvinna Till Kvinna, Front Line, 2008
http://www.frontlinedefenders.org/files/en/Insiste%20Resiste%20Persiste%20Existe.pdf

Operational Security Management in Violent Environments (Revised Edition), Humanitarian Practice Network, 2010, http://www.odihpn.org/report.asp?id=3159

Eguren E, *Protection Manual for Human Rights Defenders*, Front Line, 2005
http://www.frontlinedefenders.org/manuals/protection

Eguren E & Caraj M, *New Protection Manual for Human Rights Defenders*, Protection International, 2008
http://www.protectionline.org/New-Protection-Manual-for-Human

Bugusz W, Vitaliev D, Walker C, *Security in-a-box*, Tactical Technology Collective & Front Line. https://security.ngoinabox.org/

Easton M, Strategies for Survival: *Protection of Human Rights Defenders in Colombia, Indonesia and Zimbabwe*, Front Line, 2010
http://www.frontlinedefenders.org/node/13868

Collier, C, *Front Line Handbook for Human Rights Defenders: What Protection can EU and Norwegian and Diplomatic Missions Offer?*, Front Line, 2008
http://www.frontlinedefenders.org/files/FL_Handbook_EU_Guidelines_ENGLISH.pdf

Emergency Response Kits, Capacitar
Internationalhttp://www.capacitar.org/emergency_kits.html

Security Risk Managment - NGO Approach, Interaction Security Advisory Group,
http://www.eisf.eu/resources/item.asp?d=2551

APPENDIX 1

Example: SWOT analysis on Security

A SWOT analysis means analysing strengths, weaknesses, opportunities and threats (the acronym 'SWOT' comes from the initial letters). The strengths and the weaknesses are 'internal' (within your organisation) and the opportunities and threats are from the external environment in your region or country.

A SWOT analysis can be carried out in relation to any situation, but here is an example in relation to security.

To do a SWOT analysis:
Step 1: In a group of colleagues, use a sheet of flip chart paper divided into 4 (as below) and brainstorm the items to be included. Write up the contributions of everyone.
Step 2: Consider which are the items to be prioritised (between 3 and 5) and develop concrete action plans relating to these priorities.

Strengths (in relation to security)	**Weaknesses (in relation to security)**
• Committed staff • Senior staff are experienced in dealing with threats • Some influential contacts in Government • Independent media supports our work • Good contacts with regional and international Human Rights organisations	• Knowledge about how to deal with threats is not shared in a uniform way • No security plan for office and activities • Poor relationship with Ministry of Defence (which is responsible for the army) • Government-controlled media does not cover our activities
Opportunities (in relation to security)	**Threats (to security)**
• Other local NGOs working on human rights: advocacy; legal issues;and psychological support • European Union Guidelines on HRDs - we can approach Embassies to assist us	• Army and armed opposition group both issue threats to NGOs working on human rights • Potential legislation to control activities and funding of human rights NGOs

Prioritisation and action (example only - this organisation decided to focus on the major threats):

Priorities:

1. Programme Manager to write draft security plan and consult on it. (Completion date: 3 months time).
2. Director and senior management to meet with former colleague who now works at the Ministry of Defence to discuss a strategy for improving relationship with the Ministry (Date: next week).
3. Director and senior manager to meet with religious leader who has influence over the armed opposition group (the senior manager is a member of the religious leader's extended family) (Date: next month).
4. Organise a joint meeting with other local NGOs who may be affected by the potential legislation to control human rights NGOs to discuss joint advocacy initiatives (Date: in three weeks time).
5. Persons responsible for an overview of ensuring these activities happen and taking them forward: Director and Programme Manager.

APPENDIX 2

Example of Context Analysis Questions

1. What are the key issues in the country?	2. Who are the main actors on these key issues?	3. How might our work negatively or positively affect the interests of these actors?	4. When are HRDs most likely to be attacked (verbally or physically)?
• Political control of the country (even more delicate since revolutions in Tunisia and Egypt, and with forthcoming elections) • Polarisation – ruling party and opposition • Land use and distribution • Resource control (minerals etc) • Poverty • Unemployment • Attraction of foreign investment • Violence against opposition and HRDs	President & ruling party	Negative, HRDs seen as opposition and affecting reputation of country regarding investment	• prior to, during, post-election • working on a sensitive investigation • requesting information from the authorities on sensitive issues • after publishing challenging materials (eg statements, reports) • when your work is having impact in the region / country / region • after giving sensitive information to international bodies • at key anniversaries • at demonstrations
	Opposition	Positive generally – but some problems in violations by opposition are highlighted by HRDs	
	Army	Negative, HRDs seen as opposition & threat	
	Police	Police – negative – as army	
	Foreign states – embassies	eg 1 – negative, long relationship with president and mining interests eg 2 – European – positive, supportive but HRDs can be labelled as being under control of West Regional - supportive but not influential	
	UN agencies	Positive, supportive but cannot be too openly critical	
	International human rights orgs	Positive, supportive	
	State-owned media	State controlled - negative	
	Private media	Fighting for survival but sympathetic	
	Public opinion	Polarised	
	Judiciary	Mixed – some independence	
	Religious leaders / groups	Mixed – some support the status quo, some challenge it	
	Business interests	Business interests – want stability. May be different perceptions of what will achieve that	

APPENDIX 3

Discussing risk and threat with illiterate communities

Many illiterate communities are actively protecting their rights against threats and aggression. In these communities, the Risk Formula may not resonate with them because of its mathematical format.

One way of discussing the components of the Risk Formula was devised by Lina Selano, an HRD in Ecuador:

1. **Draw a picture in the earth of two mountains with a river running between the mountains. On one bank of the river draw the community village. At the top of one mountain is a big boulder.**

2. **Then add in to the picture a small man who is trying to push the big boulder down the mountain towards the village.**

3. **Finally, add in to the picture a large stick in the small man's hands, which he is using as a lever to roll the boulder down the mountain.**

Ask the community members:

• What are the risks (what might happen to the village and the community)?

(They may respond that there is a chance that the village will be destroyed, people injured or killed)

• Ask what the level of threat is in each of the 3 versions

(They may respond saying that the first version is only a risk if there is an earthquake, the second version is not much risk as the man cannot move the boulder but the third version is a big risk because the man's capacities have been increased.)

Invite community members to come and draw in the picture possible solutions to situations of risk – and point out the capacities in each solution. They may suggest responses such as:

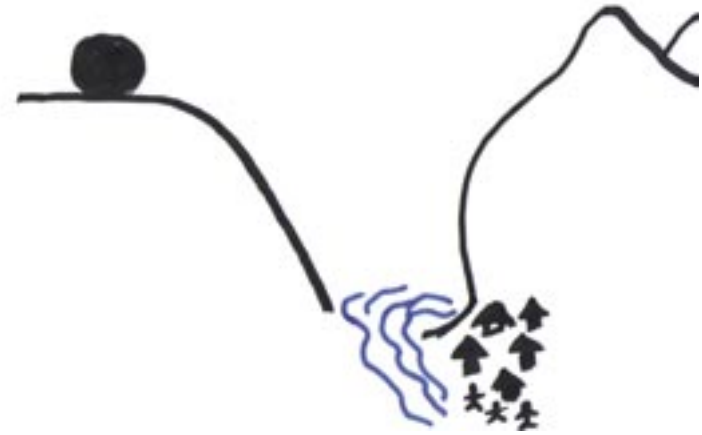
• drag the boulder to a safer place
• keep a lookout to alert the community - parrots can be trained to sound the alarm over a wide area in response to a special noise or signal
• plant trees or cactus to impede the progress of the boulder if it rolls down the mountain
• escape in canoes down the river
• relocate temporarily to another place
• go up the mountain and escort the man away, or remove his lever
• call for assistance from neighbouring communities or organisations working on human rights

You can summarise the ideas and conclude that there are different options, which might be more or less effective at different times. The challenge is to consider all the options and assess which may be most effective.

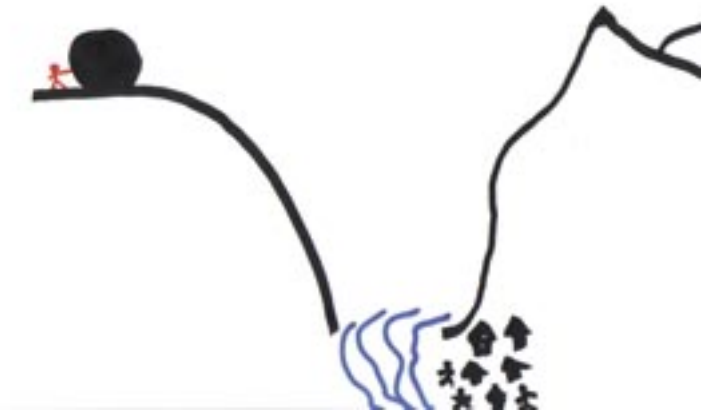
After discussing this example, turn the discussion to the issues facing the community.

How to discuss the components of the Risk Formula.
Devised by Lina Selano, an HRD in Ecuador

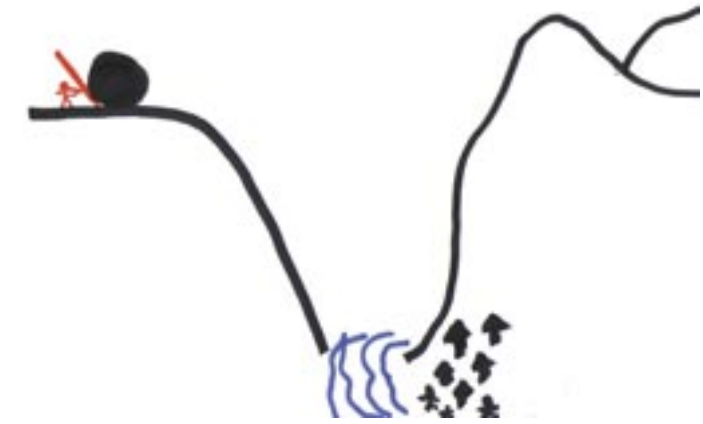
1.



2.



3.



APPENDIX 4

Check list: capacities identified by HRDs

This check list is not intended to be a blueprint for security. Your own context is the key determining factor. Consider the risks and threats you face, and any vulnerabilities you have in order to supplement and personalise this list.

Knowledge:

- about the risks and threats facing you
- about your legal rights, your country's laws, national and international remedies
- about your community, culture and political system
- about how to deal with stress

Contacts:

- Supportive local community
- Capacity to mobilise large numbers of people quickly
- Local contacts – human rights organisations, media, and influential figures
- Contacts in the government, police and other key actors
- Contacts in Embassies (particularly European Union and Norwegian Embassies) which have specific guidelines for the protection of HRDs (see Front Line Handbook for Human Rights Defenders – What protection can EU and Norwegian Diplomatic missions offer?[1])
- Regional and international human rights networks and organisations[2]

Planning:

- Security plans for every day risks
- Contingency plans in case the worst risks materialise
- Emergency plan (in the event of unexpected risk materialising)
- Clear responsibilities for security
- Mainstreaming security in work plans
- Regular reviews of security plans

Organisation / office:

- Good public reputation
- Relevant physical security - gates, locks, secure doors and windows, safe, good lighting etc
- Clear organisational mandate (so it can be explained quickly to others, eg at a checkpoint)
- Supportive environment for discussing risks
- IT security (eg firewall, anti-virus and malware protection , password system, risks of internet cafes, safe email addresses, encryption of documents)
- Clear systems for handling sensitive information
- Visitor policy to prevent unauthorised access

Other:

- Own behaviour - living within the law
- Supportive family
- Access to a safe house if required
- Safe transport
- Financial resources
- Health insurance
- Ability to manage stress

Vulnerabilities are a lack of these capacities – consider what you need to develop.

1. http://www.frontlinedefenders.org/files/FL_Handbook_EU_Guidelines_ENGLISH.pdf
2. See Appendix 17 List of useful organisations for HRDs

APPENDIX 5

Check list: Office Security

This check list is not intended to be a blueprint for security. Your own context is the key determining factor. Consider the risks and threats you face, and any vulnerabilities you have in order to supplement and personalise this list.

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 bounderies (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
   - Do you have a special 'safe' room?
   - Can the sign with your office name on it be taken down in times of increased threat to reduce your vulnerability to attack?

3. Office personnel
   - Do you recruit only trustworthy people, including guards, and take up their references?
   - Are all personnel trained in the relevant security plans?
   - Do you have a plan in case the office is raided by the authorities, or other groups?
   - Do you operate a 'need-to-know' policy about the most sensitive work?
   - Do you maintain good dialogue with all staff, especially if you know they have financial problems or are under other pressures? (Disgruntled staff can make dangerous enemies.)
   - When someone leaves the organisation, do you change security measures, passwords, keys as appropriate?

4. Visitor Admission procedures and 'filters'
   - Are admission procedures in operation for all types of visitors? Are all staff familiar with them?
   - Do ask those staff members who usually carry out admission procedures if the procedures are working properly and what improvements are needed
   - Do staff know what to do if an unexpected parcel arrives? (eg isolate it, do not open, call authorities)
   - Do you note the names of visitors (including those attending meetings at your office)? If yes, is this information sensitive and how do you protect it? (for example by codes or encrypted files)

5. Information security (see also Appendix 14, Computer and Phone Security)
   - Do you carry out regular back-ups and keep the back-ups in a safe place outside of the office?
   - Do staff know not to leave any sensitive information on their desks?
   - Do you have a secure system for recording confidential information, eg about clients or witnesses?
   - Do you give your (physical and electronic) sensitive files secure names so they are not immediately identifiable?

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

7. 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?

APPENDIX 6

Check list: Home Security

This check list is not intended to be a blueprint for security. Your own context is the key determining factor. Consider the risks and threats you face, and any vulnerabilities you have in order to supplement and personalise this list.

- Use the best protection measures you can afford and those which are normal in your community – if you have unusual security measures you may make others more suspicious of you. Consider: locks, bars, gates, fences, spyhole, alarms, CCTV, good lighting around your house etc
- Keep emergency numbers by the phone – police, ambulance, fire services, and also the numbers of colleagues / allies to be called in an emergency
- Have fire alarms, fire extinguishers and first aid kit available
- Have separate entrance and emergency exit if possible
- Consider the safety of our car parking area - could anyone plant a surveillance or explosive device? If yes, you need to have a checking routine
- Tell family members and any staff not to accept unexpected packages in case of explosives
- Invest time and effort in developing good relations with your neighbours. Trusted neighbours could alert you to anything suspicious in the neighbourhood (cars, people asking questions about you etc) and give you an escape route through their property
- Discuss with your family as far as possible what the risks are: have plans in place for what to do in case certain risks materialise
- Spouse: some HRDs tell their spouse everything about the risks they face (and what the spouse should do in different security situations); some tell them nothing, believing that ignorance of the risks will protect the spouse. Consider what is best for you – secrecy can damage relationships
- Children: consider what you can tell them and how you can prepare them in a way which will keep them safer but not scare them - include telling them not to talk to strangers - including those asking questions or go with any strangers
- Consider having a code for a sudden danger such as “go and play with your [name of toy]” means ‘run to your auntie’s house.’
- Teachers: develop a good relationship with your childrens’ teachers and tell them that only authorised people can pick up your children
- Staff (domestic worker, driver, guard etc): only hire trusted people and train them to
  - report anything suspicious – unusual vehicles or people in the area
  - not to let any person into your home without your permission
  - to check (by phoning the office) of any repair workers who say they need access to the premises, eg phone repairs, electricity, water. Do not let such people out of their sight whilst on the premises
- Consider having a simple Emergency ‘Traffic Light’ system to code the situation:
  - Green = normal
  - Amber = heightened risk where special precautions are taken, eg children are taken to and from school, a guard is hired
  - Red = high risk where appropriate action is taken, eg family to relocate to a pre-arranged place
- Do not leave sensitive documentation at home
- Avoid taking work home if the content is sensitive
- Ensure you obey laws and regulations, eg personal taxation, rules of the road etc
- If you are invited out, do not accept drinks or food from unknown people (in case they are drugged)

APPENDIX 7

Check List: Protection Of Others (Clients / Witnesses / Survivors etc)

This check list is intended to act as a reminder of key points for HRDs when they are dealing with clients (witnesses, survivors of violence etc), who may be, or become, at risk because of their contact with you.

It does not aim to deal with their security outside of their contact with you, but you could give them this booklet and suggest they create their own security plans.

Begin your own check list by referring to the Risk Formula, and assess what are the risks, threats (if you know of any), vulnerabilities and capacities of these clients.

- Explain clearly to the client what your organisation does and what they can and cannot expect from you
- Explain to the client how much you can protect them (eg by withholding their name etc)
- Ask the client what they think are the risks in communicating with you, and respond telling them anything they might not have considered
- Communicating with clients: choose the safest possible means if you or they may be under surveillance:
  - Ideally meet face to face (see below) and arrange a simple code for communicating – eg "I'll meet you on Tuesday at 11 am" could mean "I'll meet you Monday (one day before) at 10 am" (1 hour before). Arrange the venue for the meeting at this face to face meeting.
  - Ask the client their preferred communication method (and advise them if this is not secure)
  - Phone: are you likely to be under surveillance? If so, do not say anything compromising. Skype to skype is probably a safe method, if feasible. Public phone to public phone can work for some communications if you choose phone booths that are not near your homes or offices.
  - Email: does the client have a safer email address, eg gmail or riseup.net? If not, avoid compromising language and making arrangements to meet using this method.
- Meeting clients when you may be under surveillance:
  - A busy fast food café where the tables are not pre-assigned is safest. Security may be compromised if meeting at your office, home or car or theirs. A public space such as a park could be safe but keep walking and be aware of others taking the same route, as microphones can be effective from 50 metres away.)
  - If you must meet in an office or home, avoid meeting rooms and offices. The laundry room (put on the washing machine) or corridors are less likely to be bugged.
- If you publish information based on the client's story later, check again with them what their situation is. Someone who agreed to have their name used, or photo included, may change their mind if they receive threats or the situation changes in other ways.

Note: Some HRDs have encountered people pretending to be witnesses in order to frame them or lead them into a risky situation, so check your contacts carefully.

APPENDIX 8

Demonstrations

This check list is not intended to be a blueprint for security. Your own context is the key determining factor. Consider the risks and threats you face, and any vulnerabilities you have in order to supplement and personalise this list.

Lay the foundations:

- Clear purpose of demo – clearly communicate this to all (is there general agreement amongst likely demonstrators? If not reconsider action)
- Identify best place (for impact, for security, etc.)
- Security analysis:
  - What possible opposition or disruption may there be?
  - Can the police can be relied upon to deal with any disruptions. If they can't, consider if a demonstration the best way to make your protest

Teamwork:

- Allocate responsibilities, eg:
  - Media strategy (including video footage and social media alerts such as Facebook) and spokespeople
  - Police liaison
  - Supporter liaison (including identifying people who can act as ears to the ground for hints of unrest/opposition to the demonstration)
  - Liaison with any international organisations who may be of help
  - Legal advice – is a lawyer available in case of arrests?
  - Security coordinator (responsible for judgements on overall security – including cancelling the demo if need be – steward training, mapping the area and organising escape routes etc)
  - Message coordinator (banners, flyers, speakers)
  - Medical support (at least knowing the nearest medical facilities)

In advance:

- Gain permission of the authorities (even if you have, have lawyers prepared who know the local steps for appealing a ban which may happen at the last moment)
- Liaise with police as early as possible regarding safety concerns, the plans on both sides, and identify the liaison people
- Get megaphones, microphones etc
- Invite impartial observers to observe the demonstration
- Survey demonstration route
- Train stewards on the route, destination and timetable for demo, any conditions laid down by the authorities, how to disperse participants safely at the end, who to contact in case of critical events (they should not tackle disruptive people themselves), and equip them with communication devices and identification (such as t-shirts or armbands)
- Plan protective clothing – eg leather jacket in case of assault, and shoes you can run in
- Consider organising the demonstrators in groups of 4 – everyone should look out for each other in this group so you can more easily identify later if anyone has been arrested
- Have lookouts overlooking the demo from vantage points to identify any trouble spots to security coordinator
- If you are expecting infiltration from disruptive elements, consider enclosing your demonstrations in a human chain (people on the outside of the mass of demonstrators all link arms to prevent interlopers joining in)

During the demo:

- Communicate to crowd what is happening, when (people can get frustrated if they are waiting a long time or are unsure what is going on)
- Have lookouts on routes towards the demo to alert the security coordinator if disruptive elements emerge
- Do not have all your key people at the demo – the international liaison, legal advisor etc should be situated in a nearby office
- Be prepared to abort the demonstration if circumstances demand this.

Adapted from: *Prides against Prejudice, a toolkit for pride organising in a hostile environment, ILGA-Europe.]*

APPENDIX 9

Check list: Detention / Arrest / Abduction / Kidnap

This check list is not intended to be a blueprint for security. Your own context is the key determining factor. Consider the risks and threats you face, and any vulnerabilities you have in order to supplement and personalise this list.

Arrest or detention (by the authorities) and kidnap or abduction (by the authorities or other group) are separate risks, but they have some elements in common. Therefore it is worth looking at these risks together.

NB: Detention in this check list also covers arrest. Abduction and kidnap are similar but in the case of kidnap, a ransom or demand is made.

Arrest / Detention

1. If you are at risk of arrest, secure the services of a lawyer in advance if at all possible (there are some strategies below from HRDs who live in countries where lawyers are not guaranteed the right to meet their clients)
2. Memorise your lawyer's telephone number – your mobile phone may be taken from you but there may still be an opportunity to make a phone call
3. Know your rights (eg telephone call, family to be informed etc) and request them firmly
4. Know the law – eg a witness is required to answer questions; a suspect is not required to reveal anything which may incriminate them
5. Ask those detaining you for the precise reason for your detention. Ask for your current location (if not known)
6. Do not answer any questions without the presence of your lawyer
7. Carry any necessary medication with you at all times
8. When you are arrested, have a colleague to accompany you, if possible
9. Have a security contact who will take measures to find you if you do not check in at certain times during the day and knows where you might be taken if arrested
10. Do not resist arrest – you could be assaulted and charged with more offences

Here are some strategies HRDs have used in countries where they were not allowed to meet with lawyers:

"I sent a message on Twitter and Facebook and 50 people turned up outside the police station - the police wanted to arrest me secretly so they let me go." HRD, Asia

"I said 'I feel ill, I just can't remember anything." HRD, Middle East

"I just deny everything – I think once I admit something I might be abused to get more information"

HRD, Africa

"When I saw the police arriving, I rang a friendly contact in the media who publicised my detention, and I was later released." HRD, Asia

Abduction / Kidnap

The context here is key. You should know in advance if there is a risk of abduction / kidnap, who is at risk, the behaviour of kidnappers and how kidnaps in your area have been resolved.

Your protection strategies to avoid abduction / kidnap will include:

1. Develop local contacts who can warn you about heightened risks
2. Develop influential local contacts who could protect you (eg you could use their name if abducted, they could be called upon to mediate with the kidnappers)
3. Always act on local advice
4. Practise situation awareness:
   - if you are going to be abducted, you are likely to be under surveillance by the abductors

before being taken. They will probably know where you work and where you live and follow you – be alert to any signs of surveillance (see also Appendix 11 – Check list : Surveillance)
- if you are under surveillance anyway, an indication that an abduction is planned may be more open surveillance and more people following you
- if you have a good relationship with your neighbours (at work and at home), they may alert you to suspicious activities
- empty markets, deserted roads etc could be a sign of activity by armed groups

5. Only let trusted contacts know your travel plans. Avoid routines.
6. Blend in as much as possible – consider which is the safest method of transport to do so, and how to dress to avoid attention
7. Have a security contact who will take measures to find you if you do not check in at certain times during the day
8. In times of heightened risk, take steps not to be alone

What do do while being abducted / kidnapped

1. Stay calm* and quiet (the kidnappers may be nervous and inexperienced – your behaviour could trigger violence). It does not make sense to shout or struggle unless you reasonably expect that these tactics will ensure your rescue
2. Do not try to escape – unless you are certain you are going to be killed. If you are able to fight back, aim to do the attacker maximum damage (eg kick in the groin, poke in the eye) so that he cannot run after you easily.
3. Be careful about eye contact especially during tense moments: eyes can show fear, anger or contempt which can trigger violence. Face your captors (it is more difficult to harm someone who is facing you) but avoid making eye contact
4. If you are in a group, try not to be separated from the group
5. If there is a rescue attempt by force, drop to the floor, seek cover and keep your hands over your head

* You can use deep breathing techniques: breathe into the abdomen for 4 counts, out for 4 counts, and/or recite a prayer, mantra or affirmation

Surviving the kidnap period – relations with the kidnappers

1. Try to gain the kidnappers' respect and build rapport with them
2. Avoid talking about controversial topics; an excellent topic is family and children
3. Obey orders without appearing servile
4. Avoid surprising, alarming or threatening your captors; don't indicate that you would testify against them
5. Be cautious about making suggestions to your captors, as you may be held responsible if something you suggest goes wrong
6. If there are several people kidnapped, elect one spokesperson to speak for the group. This presents a common front and avoids the kidnappers playing you off against each other
7. Regard all information they give you with scepticism
8. Ask for permission to call your organisation to let them know you have been kidnapped. Do not call without permission
9. 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 by your captors
10. You may develop some sympathy with your captors' cause, but remember this does not justify your abduction.

Surviving the kidnap period – physical and mental health

1. It is normal to feel extreme shock and depression
2. Accept that you may be held captive for a long period of time. Try to keep a record of the days
3. Inform your captors of any medical treatment you have been receiving
4. Take care of your health by eating (even if the food you are offered is unappealing),

developing an exercise routine, and prayer/meditation

5. Keep your mind occupied. If books or writing materials are not available, pray, meditate, recall favourite books and films, compose music, plan for the future in your head – all this can lift your mood
6. Keep your environment clean and tidy, ask for adequate washing and toilet facilities
7. Be mentally prepared for changes: of location, or guards, being separated from others
8. You may be treated in a humiliating or terrifying way. Fear of pain or death are normal reactions – do not lose hope
9. Know that your organisation has a Crisis Management plan and is doing everything in its power to get you released

Release

1. During the initial kidnap and during release are the most tense times for the kidnappers. Stay calm and obey orders exactly, but also:
2. Stay alert - you may need to make a run for it
3. Be prepared for delays and disappointments
4. Do not try to interfere with negotiations for your release
5. Try not to allow your kidnappers to exchange clothes with you: you could be mistaken for a kidnapper and attacked
6. If there is a rescue attempt by force, drop to the floor, seek cover and keep your hands over your head

Contingency Plan for Abduction / Kidnap

If abduction / kidnap is a threat, all organisations should have a contingency plan in case one of their members is kidnapped. This could include the following:

1. Everyone knows (and memorises the phone number of) the key person to contact if they believe they may be abducted / kidnapped
2. The organisation sets up a crisis committee with key roles designated in advance, such as:
   - description of the abduction, names and other details of those involved, time, date, location
   - establishing as far as possible where the person is being held and by whom (with independent verification as far as is possible)
   - person authorised to talk to the kidnappers, if they contact you (have a recording device available for phone calls)
   - contact with influential people who may be able to assist with negotiations
   - dealing with the authorities if appropriate
   - contact with and support of the family
   - contact with local, regional, national, international human rights groups if appropriate
   - media spokesperson - primed with a careful media strategy if news of the kidnapping has leaked out
   - developing a plan of support (need for medical treatment, recuperative leave, counselling and other services) for the member when released/returned home (to be implemented in direct consultation with the member and/or their family).
   - keeping other staff informed, as appropriate
   - offering psycho-social support to affected colleagues as required
3. Post crisis: Conduct a debrief and evaluation of whether the steps taken to prevent the abduction were sufficient and how the organisation could improve its reaction to the situation.

APPENDIX 10

Check list: Risk of Assault, including sexual assault

This check list is not intended to be a blueprint for security. Your own context is the key determining factor. Consider the risks and threats you face, and any vulnerabilities you have in order to supplement and personalise this list.

General:

- Do your risk analysis – consider when you may be at most risk of assault, where attacks are most likely to occur, who the perpetrators might be and what their methods would be. Your protection plan will differ according to variables such as these
- Being alone increases the risk – do not go out alone when you are most at risk and avoid the places where you are most at risk
- Use the safest transport options
- Do not carry weapons – these could be used against you by an attacker and used as an excuse by the authorities to arrest you
- Carry a whistle to blow to alert attention
- Practice screaming for help – many people 'freeze' when attacked (and their throats feel constricted)
- If attacked, use what is at hand, eg throw sand in your attacker's face
- Keep fit and always wear comfortable shoes – running is often the best form of defence
- If you are going to an event such as a demonstration where you might be beaten, wear protective clothing such as a leather jacket, and pack cardboard under your clothes
- Consider who the perpetrators might be – can you devise a believable protection strategy, such as 'I am a friend of ...(an influential person)'?
- Prepare yourself to give up valuables without a struggle
- Avoid being an attractive target by walking confidently and not displaying expensive jewellery or equipment (phones, laptops etc)
- Know where you are at all times and where you could run for help
- Have medical insurance

Sexual assault (in addition to the above):

- There are 3 basic ways to deal with this situation and you may not know what you would do until it happens. If you cannot run immediately, the options are to fight back and run, to reason with the attacker, or to submit
- If you are able to fight back, aim to do the attacker maximum damage (eg kick in the groin, poke in the eye) so that he cannot run after you easily. If you have fought back but do not escape, the perpetrator may be more violent towards you as a result
- Prepare yourself psychologically – if the worst happens, know that the perpetrator cannot deprive you of your essential self - during the attack concentrate on mentally separating your mind from your body
- Consider who the perpetrator may be – can you devise an effective protection strategy such as 'I have my period'? (If this could work, be prepared to wear a soiled sanitary towel as 'evidence') (One HRD told the attacker 'Ýes, I'd like to have sex with you but it's my period now – I can come back tomorrow'... and she was allowed to leave)
- If you are at risk of rape, consider carrying condoms (which you could try to persuade the attacker to use) or wear a feminine condom
- If you are attacked try, if at all possible, to behave with as much dignity as you can – rapists are generally motivated by a need to have power over a victim and crying and pleading may only feed this urge
- If it is possible, try to engage with the attacker on a personal basis – for example, you could tell him that he may have a sister/mother/daughter or brother/father/son your age and how would he feel if this happened to her or him?

If a colleague is assaulted, including sexual assault:

- Get the person to a place of safety where they can receive medical treatment. In the case of rape, anti-retrovirals (to avoid HIV infection) need to be taken as soon as possible and certainly within the first 72 hours. Anti-biotics and the morning after pill (which provokes menstruation whether or not the survivor has become pregnant) may also be taken
- Photograph their injuries for evidence if appropriate (and keep the crime scene undisturbed)
- If the person wants to report the crime, check if there are specially trained officers who deal with sexual violence cases
- Support the person in reporting the attack to the authorities, but respect their views if they choose not to do so
- Arrange counselling for the person and any others involved in the situation

APPENDIX 11

Check list: Travelling to rural areas (for research etc)

This check list is not intended to be a blueprint for security. Your own context is the key determining factor. Consider the risks and threats you face, and any vulnerabilities you have in order to supplement and personalise this list.

When you travel away from your home area you are more vulnerable because of lack of knowledge about your environment. This vulnerability is compounded if you travel for the purpose of a research mission on a sensitive topic and are meeting witnesses etc.

- If this is a trip with risks, start planning in good time
- Find out exactly what the risks are and how to minimise them. (Consider: Do the benefits outweigh the risks? Are you willing to accept the risks? Do you need to go or can someone else do the task required more safely?)
- Consider the safest mode of travel and the safest route
- Consider the advantages of having accommodation in a place some distance away from your final destination (so you can go there and back relatively quickly and be out of that immediate area by the time your visit becomes known to any potential perpetrators)
- Have at least one trusted contact at the destination. Check before you go and when you arrive what are the current risks.
- Do not travel alone – depending on the destination consider who to travel with, eg
  - someone from / with knowledge of the area (language, customs etc)
  - male / female (a male or female companion may be safer for cultural reasons, or as a cover for your travel)
  - special knowledge
- Have a clear distribution of tasks and responsibilities
- If you have a driver, ideally this should be a trusted and knowledgeable person
- Have an Emergency Contact person who knows what to do if there is a security crisis.
- Give the Emergency Contact a clear itinerary (your route, your accommodation, who you are meeting where, when and for what purpose). Include contacts along your route who can be trusted to assist you (names, contact details, location and background details). Do not deviate from the schedule without informing your Emergency Contact.
- Agree the schedule of checking in with your Emergency Contact, eg twice a day (or whatever is realistic, given your resources and the infrastructure), plus an emergency code word in case of crisis.
- Mechanical check of the vehicle before you go
- Consider the papers / materials you are taking – including visual materials – such as reports, agendas etc. Could they endanger you?
- Have an escape strategy – what to do / where to go if things go wrong
- Have a plan of how to transport sensitive information such as interviews, photos etc (eg in a USB

in your sock? emailed to your organisation and then deleted?)

- Take with you:
  - money for emergencies (eg vehicle breakdown)
  - maps
  - food, water
  - First aid kit

- Consider taking (if useful):
  - suitable communications equipment with you - preferably at least 2 devices (mobile phones – including one unregistered phone if possible, laptops, satellite phones etc – and check them before you go)
  - video camera
  - legal documents: ID, authorisation letters as required (or documents which support your cover story)

- Consider not taking:
  - Your mobile phone, if you think you are under surveillance (leave your phone at home and get a new, unregistered one instead, if possible)
  - Papers / materials / visual materials – such as reports, agendas etc which could endanger you

- Avoid travelling after dark

- Behave responsibly – obey local laws, avoid drinking too much, etc.

APPENDIX 12

Administrative Measures against HRDs

Administrative law is one of the three basic areas of public law (the other two being constitutional and criminal law). The powers to implement administrative laws or measures (also sometimes called 'Regulations') are delegated to administrative agencies. The breaking of a binding administrative regulation normally incurs an administrative penalty.

Administrative measures are increasingly used to harass HRDs and occupy their time.

Administrative measures may be used in different ways in different countries – these are some examples.

- Charges of having unlicensed software:
  - Review all your software and delete all counterfeit software, and any other breaches of licensing agreements (eg using home edition versions on office computers). Install (free) open source software or purchase licensed software for your office.
  - Keep all receipts and boxes of licensed software

- Demands for frequent inspection of your tax records:
  - Ensure you have an excellent accountant
  - Set up meticulous record-keeping and filing systems

- Different regulations for different types of funding:
  - Check if there are different legal regulations relating to charitable donations, international financing, commercial activities and membership contributions

- Unworkable requirements for cash handling:
  - Issue an order banning cash handling within your organisation. All payments to be made only using cards and to staff personal accounts, as well as to the accounts of external experts and organisations.

- Registration of your NGO:
  - Ensure you are aware of and comply with all registration requirements, taking expert advice as appropriate

- Permits for workshops or demonstrations:
  - Know what are the legal requirements regulating such activities and comply with them or consider the risks of not doing so and plan for the consequences (eg having lawyer on standby in case of arrest, knowing where to get medical treatment if assaulted at a demonstration)
  - If possible, ensure video recording of events to have evidence of your compliance with the law (in case participants are charged with violating the law)

- Office searches
  - Know what the law is, what can be searched for
  - All staff should be aware of who to call and what to do if a permit for a search is presented

General advice:

- Know what rights are guaranteed under your country's legislation for people in administrative detention / imprisonment (access to a lawyer, right to choose the lawyer, access to doctor, right to notify family members etc). This will be useful if you are subjected to administrative detention / imprisonment for violating administrative laws.
- Make up a schedule of all reports to be submitted by your organisation to its donors and national

authorities (judicial authorities, tax authorities, statistical agencies, pension funds and social security fund, etc) and stick to it.

- Keep all the records of correspondence with national authorities, postal notices of deliveries and envelopes. Keep telephone contact with regulating bodies' officials (prosecution office, internal affairs, justice authorities, tax authorities etc) to a minimum and instead forward replies and document copies by special delivery post (at a later stage it could be impossible to prove what had been said in a telephone conversation).

- Prepare action plans for emergencies: ask your staff to sign to show that they have read them

- Make sure that there is no conflict of interests: such as contracts between your organisation and founders, members, partners or close relatives of the organisation management.

- Discuss regularly with other NGOs what types of harassment they receive, and how they protect themselves

APPENDIX 13

Check list – Defamation of HRDs

This check list is not intended to be a blueprint for security. Your own context is the key determining factor. Consider the risks and threats you face, and any vulnerabilities you have in order to supplement and personalise this list.

Consider the context of the defamation. Is it a one-off occurrence? If you respond, will it increase the circulation of the defamation? Is it pervasive and increasing in intensity? What will be the impact of the defamation on you and your organisation? Depending on your analysis of these questions, you can consider how best to react.

Discuss the defamation with trusted colleagues and consider the best response - the support of your organisation is important.

Any rebuttal you disseminate should refute the allegation point by point, with facts. Do not mount a counter-attack.

Options:

- Ignore the defamation
- Inform all your colleagues, supporters, donors etc of the truth
- Get legal advice
- Rebut the defamation in the most relevant way
- If the defamer is known, discuss with them the untrue allegations, or commence a mediation process with a trusted intermediary
- Report it to the police and, if the perpetrator is known, make a case against them
- In any event, monitor the situation to check if the defamation is increasing

Here are some specific suggestions in addition to those above:

- Defamation on the internet - websites, social networking sites, blogs etc
  - request the moderator / administrator to remove the defamation
  - or respond to it on the same site, giving the facts
  - publish a statement on your website / blog etc refuting the allegations
  - consider making a legal case against the perpetrator

- Defamation in leaflets
  - produce a leaflet with the true facts and distribute it in the same places

- Public statements
  - hold a press conference, radio interview etc rebutting the allegations
  - send out a press release with the true facts signed by influential supporters of yours, eg well-respected figures, human rights organisations

Finally, consider if you need psychological support at this stressful time.

APPENDIX 14

Computer and phone security

This check list is not intended to be a blueprint for security. Your own context is the key determining factor. Consider the risks and threats you face, and any vulnerabilities you have in order to supplement and personalise this list. It is also just a list of key points.

See Security-in-a-box https://security.ngoinabox.org/ for much more detailed information.

This information includes a number of the tips to be found in the Awareness Cards of the *Security-in-a-box* project – see the link above.

1. Protect your computer from malware and hackers

- Install antivirus software, anti-spyware and a firewall
- Do not use pirated software – it leaves you vulnerable due to lack of updates and to charges of possession of illegal software
- Consider using FOSS (Free Open Source software) such as AVAST anti-virus, Spybot anti-spyware and Comodor Firewall
- Consider using a safer browser like Firefox which has built-in security

  (see https://security.ngoinabox.org/en/chapter-1 for more information on how to protect your computer)

2. Create and maintain secure passwords

- The longer your passwords the better. Your passwords should be longer than 12 characters, contain upper and lower case letters, numbers, and special characters, and a space if possible.
- Your passwords should preferably not contain dictionary words and/or publicly available information about yourself such as birthday or friend's name – jumble up the words or replace words with special characters or numbers, or mix languages
- Consider using a phrase as your password – this can be a title of a book or an extract from a song (with characters or numbers substituted for letters)
- Change your passwords often
- Have strong different passwords for different services, update them regularly and do not share passwords (consider using KeePass to store all your passwords – see https://security.ngoinabox.org/en/chapter-3 for more information on KeePass)
- NEVER share your passwords
- NEVER let websites and programs store your passwords

  (see https://security.ngoinabox.org/en/chapter-3 for more information on secure passwords)

3. How to protect sensitive files on your computer

- Backup your files regularly and store the backup in a safe place
- Hide sensitive files with innocuous file names
- Consider encrypting your files (although encryption is illegal in some countries and could draw attention to you)
- A FOSS application called TrueCrypt can both encrypt and hide your file
- Deleted files can still be retrieved from your computer by an expert – consider using a secure deletion tools such as CCleaner (to wipe temporary files) and Eraser
- If possible check the reputation of your ISP or the place where you plan to connect to the internet, such as internet cafés
- Make sure the people you communicate with are also privacy and security aware. Communication is a two-way process. It does not make sense if only one party is concerned with privacy and security.

  (see https://security.ngoinabox.org/en/chapter-4
  and https://security.ngoinabox.org/en/chapter-6 for more information)

4. Keep your Internet communication private

- Many webmail accounts are insecure (including Yahoo and Hotmail) and provide your IP address in the messages you send. Gmail and Riseup email accounts are more secure (although Google has in the past conceded to the demands of governments that restrict digital freedom).
- Using Internet cafés can expose you to surveillance - be very aware of the risks, and whom you are contacting with what information. Delete your password and browsing history after use.
- Use "https" instead of "http" when connecting to your online services, whenever possible, so your username, password and other information is transmitted securely
- Do not open email attachments from someone you don't know, or which look suspicious
- Be especially aware when sending, receiving and viewing sensitive information on the internet
- Consider using a proxy service or application to anonymise you on the internet. This allows you to access and communicate on the internet using another computer's IP address.
- Instant messaging (chat) is also not normally secure, although Skype is probably more secure than others

  (see https://security.ngoinabox.org/en/chapter-7 and http://security.ngoinabox.org/en/chapter-8 for more information)

5. Social networking

- Think carefully about the information you share about yourself, your whereabouts, friends etc
- Get consent if posting information, documents, pictures and the locations of others
- Make sure your passwords are secure and changed regularly.
- Be careful when accessing your social network account in public internet spaces – only use them if you are sure they can be trusted. Delete your password and browsing history after using a public browser or computer.
- Read and understand the End User License Agreement (EULA), Terms of Use and/or Privacy Guidelines documents. These documents may change in the future, so it is important to revisit them regularly.
- Make sure that you are familiar with the privacy settings of your social network account. Don't rely on the default settings – customise your settings and review them regularly as the service may make changes.
- Use caution when installing applications suggested by social networking services. Use these applications only if you trust their source, understand what information they will expose, and are able to control the outflow of your information.

  (see https://security.ngoinabox.org/en/chapter-10 for more information)

6. Mobile phone security

- The current setup and technology around mobile phones (including SMS and voice calls) are insecure – your location can be tracked and your communications intercepted, so always consider the safest way to communicate important information.
- The safest mobile phone is a cheap, unregistered, pay-as-you-go phone which you discard after use
- Activate your mobile phone's password or pin lock
- Don't save sensitive information on your phone, or if you have to, encode it
- Be continually aware of your environment when using your mobile phone, and refrain from this in risk prone places and situations
- Make sure all your information is deleted on your mobile before selling it or having it repaired
- Destroy unusable phones and old SIM cards before discarding them
- When working with individuals and organisations transmitting sensitive information, consider having separate phones and SIMs for work and personal use.

  (see https://security.ngoinabox.org/en/chapter-9 for more information)

APPENDIX 15

Surveillance Technology and Methodology

This check list is not intended to be a blueprint for security. Your own context is the key determining factor. Consider the risks and threats you face, and any vulnerabilities you have in order to supplement and personalise this list. See also the section on surveillance in Chapter 3, Analysing Threats.

Are you under surveillance?

- If you are not sure if you are under surveillance, assume you are and be very aware of what you say and do in order to protect yourself and others

- Discuss with other HRDs what surveillance methods are used in your country, what is the purpose (to collection information? to intimidate? to prepare for an abduction?) - your tactics will change depending on the objective of the perpetrators

- Discuss with your colleagues how you should react if you discover surveillance. For example if you find a tracking device on your car, should you leave it there or get rid of it?

A general rule seems to be – if you spot surveillance, pretend you haven't. If they see you are aware they will at best move further away and be harder to identify, and at worst become violent.

Dealing with surveillance technology and methodology

- **Microphones** can be microscopic and virtually undetectable by the human eye (eg in a jacket buttonhole – to tape your conversation), on a key fob (which someone puts down in on the table next to you), in a light fitting, wall or door of your meeting room, double-adapter plugs... but they need good sound quality
  - Don't hold sensitive conversations in your home, office or car. If this is not possible, choose noisy and/or unexpected places, eg laundry rooms (with the washing machine on), cleaner's closet...
  - If you are going to have somewhere swept for bugs, do not discuss it in that building, nor on the phone. Many microphones are sound-activated so do the sweep during a normal day under the guise of a normal activity such as having the room painted

- **Cameras** can be microscopic and hidden in TV screens, clocks, ornaments etc
  - Have good office and home security
  - Do not accept gifts from people you don't trust

- **Phones** can be tracked – both the sim card and the phone itself. Phone calls and text messages can be monitored. Phones could be loaded with a device or software and be used as microphones.
  - Do not leave your mobile phone unattended or lend it to people, even those you trust
  - Going to a sensitive meeting? Leave your phone at home. Or turn it off and take the battery out – ask all meeting participants to do the same
  - Skype to Skype conversations are believed to be relatively safe (but that could change...)
  - Public phone box to public phone box calls can also be relatively safe, but use different ones and never the ones nearest your home or office
  - Safest calls are from cheap unregistered Pay-as-you-go phones which are discarded after use

- **Vehicles** can have tracking devices installed on them
  - Get to know what your vehicle looks like underneath, check regularly, especially at the back of the vehicle (as the device has to communicate with a satellite)
  - Beware of who services your car, or recalls from the manufacturer to 'fix a problem'

Have a plan – if an HRD finds a device in their home or car, what should they do? Ignoring it whilst being aware of the implications and behaving accordingly could be the safest option.

Physical surveillance (being followed)

- Know that very professional surveillance operators may work completely unnoticed
- Practice situation awareness at all times (whilst resisting paranoia...):
  - describe people you see to yourself so you can recognise them again (consider who they remind you of, their height, walk - things that can't be disguised) Keep a notebook and write descriptions down as soon as practicable
  - who looks out of place? Are they wearing jackets/coats and/or carrying bags (to conceal surveillance equipment)?
  - notice vehicles - colour, make, and their occupants (perhaps they have maps, food and drink containers, are apparently talking to themselves etc)
- Don't be tempted to use the techniques you see in films (eg looking in shop windows for reflections, tying your shoelaces and looking around, speeding away from one car following you – these will be noticeable and ineffective). Instead act naturally at all times.
- All surveillance will have a 'start point' which will most likely be your home or work. Check
- Do not have a fixed routine. Vary the times and routes you use to go to work, go home, go to the gym, shopping etc.
- Align papers on your desk in a way so you know if it has been tampered with.

- **Vehicle surveillance:** a box system of 5 vehicles will probably be used – one ahead of you, 2 behind you and one to each side, perhaps on parallel roads
  - Don't bother speeding away – there is probably more than one vehicle
  - Drive naturally – don't keep moving your head to look in your rear mirrors
  - To check for surveillance, turn into a cul-de-sac or a petrol station to get fuel – but be careful that it looks natural
  - To evade surveillance park somewhere and then, in a relaxed way, jump onto public transport

- **Attending sensitive meetings:** Arrange a simple code for sensitive meetings, eg "I'll meet you on Tuesday at 11 am" means "I'll meet you on Monday at 10 am" (a day and an hour earlier)
  - Safest meeting places are noisy, popular cafés where the seats are not allocated (and microphones will be impossible to install where you are going to sit
  - When you meet face-to-face at a safe place, use the opportunity to agree codes for the future or give an encryption key

If you see an increase in physical surveillance (cars, operatives etc) and it becomes more open, it could be an indication that you are going to be detained. Do not follow your regular pattern as soon as you notice this. Consider relocation to a safe house.

Finally:

Many people innocently reveal information about themselves and their whereabouts, through:

- business cards (have one with your mobile phone number and safe email address which is only given to trusted friends)
- Facebook or other social networking sites – your profile can reveal your vulnerabilities and reveal where you are, who you are with...

APPENDIX 16

Overcoming Resistance to Security Planning in your Organisation

The following text is reproduced with thanks from Chapter 2.3, *New Protection Manual for Human Rights Defenders*, Enrique Eguren and Marie Caraj, published by Protection International, 2009.

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 exposed 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.

COMMON RESISTANCE STEREOTYPES	REASONING BEHIND THE STEREOTYPES	RESPONSES TO OVERCOME RESISTANCE
"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."	"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."	• 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 homogeneous 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.

APPENDIX 17

Selected International and Regional Organisations providing support to HRDs

Organisation	What They Do	Address	Website
American Jewish World Service	AJWS is dedicated to alleviating poverty, hunger and disease among the people of the developing world regardless of race, religion or nationality. Funds grassroots organisations working for more just societies.	American Jewish World Service 45 West 36th Street New York, NY 10018	http://ajws.org/contact_us.html
Amnesty International	Amnesty International is a worldwide movement of people who campaign for internationally recognized human rights for all. Has a small programme to protect HRDs at extreme risk.	1 Easton Street London WC1X 0DW, UK	http://www.amnesty.org
Arab Human Rights Fund	A not-for-profit philanthropic organization that provides financial support for the promotion and realisation of all human rights in the Arab region.	See website	http://www.ahrfund.org
The Arab Program for Human Rights Activists	Conferences, seminars, workshops, campaigns and urgent actions relating to reform in the Arab World.	10 Rue St-Sadiq of Osama Gamal El-Din Qasim seventh floor Apt 16 Behind Serag Mall, Eighth District Nasr City, Cairo	http://aphra.org
The Arab Organization for Human Rights	Carries out fact finding missions to verify human rights developments in the Arab region. Works to release political prisoners. Receives complaints from individuals and organisations and contacts the authorities. Can offer legal and financial assistance.	Main address: SG: Mohsen Awad, 91 El-Marghany Street, Apt 7-8, Heliopolis, 11341, Cairo, Egypt (Branches in 19 countries & territories – see website)	http://www.aohr.net/
The Arabic Network for Human Rights Information	Focus on freedom of expression. Human rights advocates program provides grassroots leaders with the tools, knowledge and access to promote the realization of human rights and strengthen their organisations.	See website	http://www.anhri.net
Article 19	Works on freedom of expression and freedom of information. Undertakes litigation in international and domestic courts on behalf of individuals or groups whose rights have been violated. Provides legal and professional training.	Article 19, 60 Farringdon Rd, London, EC1R 3GA, UK	http://www.article19.org/
ASHOKA	Supports social entrepreneurs financially and professionally and brings communities of social entrepreneurs together.	Ashoka Global Headquarters 1700 North Moore Street, Suite 2000 (20th Floor), Arlington, VA 22209, USA	http://www.ashoka.org
ASEAN (Association of Southeast Asian Nations) Intergovernmental Commission on Human Rights	Intergovernmental Commission on Human Rights	See website	http://www.asean.org/22769.htm
Asian Centre for Human Rights (ACHR)	Protection of human rights in Asia. Work includes increasing the capacity of HRDs and civil society groups through trainings on national and international human rights procedures; providing legal, political and practical advice for HRDs.	Asian Centre for Human Rights, C-3/441-C, Janakpuri, New Delhi - 110058, India	http://www.achrweb.org/
Asian Forum for Human Rights and Development (FORUM-ASIA)	Regional human rights organisation committed to the promotion and protection of all human rights. Work includes protection for Asian HRDs at risk.	See website	http://www.forum-asia.org/

Organisation	What They Do	Address	Website
Asian Human Rights Commission (AHRC)	An independent, non-governmental body promoting the realisation of human rights in the Asian region. Protects and promotes human rights by monitoring, investigation, advocacy and solidarity actions.	Asian Human Rights Commission, Unit 701A, Westley Square 48 Hoi Yuen Road Kwun Tong, KLN Hong Kong, China	http://www.humanrights.asia/
Avocats sans frontiers (ASF)	Legal and other assistance for HRDs at risk	ASF's HQ (Belgium) Rue de Namur 72 Naamsestraat 1000 Brussels, Belgium	http://www.asf.be/
Cairo Institute for Human Rights Studies (MENA)	Promotes respect for the principles of human rights and democracy in the Arab Region as well as engaging in dialogue between cultures. Assists with professional development for Human Rights Defenders.	Tel: +32 2 223 36 54 Email: info@asf.be 21 Abd El-Megid El-Remaly St., 7th Floor, Flat no. 71, Bab El Louk, Cairo.	http://www.cihrs.org/english/newssystem/articles.aspx?id=10&pagenumber=5
Civil Rights Defenders (Europe)	Defend civil and political rights and empower HRDs at risk in Europe	See website	www.civilrightsdefenders.org
Committee to Protect Journalists	Defends the rights of journalists and intervenes when journalists are in trouble.	330 7th Avenue, 11th Floor, New York, NY 10001, USA	http://www.cpj.org/
Council of Europe	Within the Council of Europe, the Commissioner for Human Rights promotes respect for human rights in 47 Council of Europe member states. Protection of HRDs at core of this mandate.	Office of the Commissioner for Human Rights Council of Europe F-67075 Strasbourg Cedex FRANCE	http://www.coe.int
East and Horn of Africa Human Rights Defenders Project (EHAHRDP)	Seeks to strengthen the work of HRDs throughout the region by reducing their vulnerability to the risk of persecution and by enhancing their capacity to effectively defend human rights.	See website	http://www.defenddefenders.org/
El Nadim Center for the Rehabilitation of Victims of Violence and Torture (MENA)	Provides psychological management and rehabilitation to victims of torture from Egypt and the region.	3A Soliman El-Halaby Street – Ramses Cairo, Egypt	http://www.alnadeem.org/en/node/23
Euro-Mediterranean Foundation of Support to Human Rights Defenders (MENA)	Provides financial assistance and support to local, national and regional human rights NGOs and institutes, and individuals who promote, support, protect and monitor human rights in the region.	c/o EMHRN, Vestergade 16, 2nd floor, DK-1456 Copenhagen K, Denmark	http://www.emhrf.org/
Fojo Safe House	The Fojo Safe House is funded under Sweden's Special Initiative for Democratisation and Freedom of Expression and aims to offer journalists under severe threat shelter for a short period.	Gröndalsv. 19, Kalmar, Sweden	http://www.fojo.se
Ford Foundation	Works mainly by making grants or loans that build knowledge and strengthen organisations and networks.	Ford Foundation 320 East 43rd Street, New York, N.Y. 10017 USA	http://www.fordfound.org
Freedom House	Freedom House is an independent watchdog organization that supports the expansion of freedom around the world. Supports democratic change, monitors freedom, and advocates for democracy and human rights.	1301 Connecticut Ave, NW Floor 6, Washington DC 20035, USA	http://www.freedomhouse.org

Organisation	What They Do	Address	Website
Front Line	Front Line works to protect human rights defenders at risk. Programmes include advocacy, protection, grants to increase security, training and networking.	Front Line – The International Foundation for the Protection of Human Rights Defenders Grattan House, 2nd Floor, Temple Rd, Blackrock, Co Dublin, Ireland	www.frontlinedefenders.org
European Union	Funding for human rights organisations and protection activities for HRDs through partner organisations – see website. Issued EU Guidelines for the Protection of HRDs	See website	http://ec.europa.eu/europeaid/how/finance/eidhr_en.htm http://ec.europa.eu/europeaid/what/human-rights/human-rights-defenders_en.htm
FIDH	FIDH supports HRDs and created the Observatory for the Protection of Human Rights Defenders in partnership with the World Organisation Against Torture.	See website	http://www.fidh.org
Fund for Global Human Rights	Supports frontline organisations. Dispenses grants to support campaigns that otherwise might falter for lack of resources.	Fund for Global Human Rights. 1666 Connecticut Avenue NW, Suite 410, Washington, D.C. 20009. USA	http://www.globalhumanrights.org
Hisham Mubarak Law Centre (MENA)	Provides legal advice on human rights issues in Egypt and MENA.	See website	http://www.hmlc-egy.org/english
HIVOS	Hivos contributes to a world with equal opportunities for people to develop their talents. Hivos offers financial support and by advising, networking, advocacy, providing education and exchanging knowledge.	See website	http://www.hivos.nl/eng
Human Rights First	We provide a lifeline for international human rights activists whose lives are at risk and we advocate on their behalf with US policy makers, the public, and their governments.	New York Office, Human Rights First, 333 Seventh Avenue, 13th Floor, New York, NY 10001-5108	http://www.humanrightsfirst.org/
Human Rights House Network	Protects and supports HRDs and their organisations in 15 countries in Western Balkans, Eastern Europe and South Caucasus, East and Horn of Africa, and Western Europe	Human Rights House Foundation, Kirkegata 5, 0153 Oslo, Norway	http://humanrightshouse.org
Human Rights Watch	HRW focuses international attention on human rights violations, using rigorous, objective investigations and strategic, targeted advocacy.	Human Rights Watch 350 Fifth Avenue, 34th Floor, New York, NY 10118-3299, USA	http://www.hrw.org
IFEX (International Freedom of Expression Exchange)	Exposes free expression violations around the world including alerts on journalists, writers and free expression advocates. Advice, training, financial and technical support for members plus support for campaigns on freedom of expression.	555 Richmond St. West, Suite 1101, P.O. Box 407, Toronto, ON, M5V 3B1, Canada	http://www.ifex.org
Inter-American Commission on Human Rights (Organization of American States)	Promotes the observance and the defence of human rights. Investigates individual petitions on human rights violations and recommends measures to protect human rights to member states.	1889 F St, NW, Washington, DC 2006, USA	http://www.cidh.oas.org
INTERIGHTS, the International Centre for the Legal Protection of Human Rights	INTERIGHTS works to promote respect for human rights through the use of law by providing legal expertise to lawyers, judges, human rights defenders and other partners.	Lancaster House, 33 Islington High Street, London N1 9LH, UK	http://www.interights.org
Media Defence Initiative	The Media Legal Defence Initiative exists to help journalists and media outlets defend their rights. They do this by providing financial assistance to pay legal fees, helping to access free legal advice and taking on cases in international courts.	3rd Floor Cambridge House, 100 Cambridge Grove, London, W6 0LE United Kingdom	http://www.mediadefence.org/

Organisation	What They Do	Address	Website
Office of the United Nations High Commissioner for Human Rights (OHCHR)	Provides assistance to help implement international human rights standards on the ground.	OHCHR, Palais Wilson 52 Rue des Pâquis CH-1201 Geneva, Switzerland See website for details of country and regional offices	http://www.ohchr.org/EN/AboutUs/Pages/ContactUs.aspx
OMCT (World Organisation Against Torture)	Has HRD programme including urgent interventions, materials assistance and training. Created the Observatory for the Protection of HRDs with FIDH.	OMCT International Secretariat PO Box 21 8, rue du Vieux-Billard CH-1211 Geneva 8 Switzerland	http://www.omct.org/index.php?&lang=eng
OSCE – Organization for Security and Co-operation in Europe	Regional security organisation with 56 States from Europe, Central Asia and North America. Works on early warning, conflict prevention, crisis management and post-conflict rehabilitation. Databases with resources for HRDs.	OSCE Secretariat Wallnerstrasse 6 1010 Vienna Austria	www.osce.org
OSCE – Focal point for HRDs	The Focal Point seeks to promote and protect the interests of HRDs. Organises education and training, in order to improve expertise in human rights standards, and develop monitoring and advocacy skills. Useful databases & other resources.	OSCE Secretariat Wallnerstrasse 6 1010 Vienna Austria	http://www.osce.org/odihr/44936
OSI (Open Society Institute)	Promotes tolerant democracies with accountable governments and makes grants, fellowships and scholarships available.	400 West 59th Street New York, NY 10019, U.S.A.	http://www.soros.org
OSISA (Open Society Initiative for Southern Africa)	OSISA's mission is to initiate and support programmes working towards open society ideals, and to advocate for these ideals in Southern Africa.	See website	http://www.osisa.org
OSIWA (Open Society Initiative for West Africa)	Advocacy and grant making foundation for West Africa	See website	http://www.osiwa.org/
OSIEA (Open Society Initiative for East Africa)	OSIEA promotes public participation in democratic governance, the rule of law, and respect for human rights by awarding grants, developing programs, and bringing together diverse civil society leaders and groups	See website	http://www.soros.org/initiatives/osiea
Peace Brigades International (PBI)	Provides accompaniment for HRDs and communities whose lives are threatened by political violence (as of July 2011 in Colombia, Guatemala, Mexico and Nepal)	See website	http://www.peacebrigades.org/
Protection International	PI mobilises the national and international community to protect HRDs and provides HRDs with training and tools. PI Protection Desks exist in some countries - see website.	11 Rue de la Linière, B1060 Brussels, Belgium	http://www.protectioninternational.org/
REDHAC, Network of Human Rights Defenders in Central Africa	Protection of HRDs in Central Africa	Région du Littoral, Ville de Douala, Ancienne Rue Makumba, Immeuble Lux Optique 2e Etage - Face Auto Ecole Jojo, Cameroun	http://www.redhac.org/
Reporters Without Borders	Defends journalists and media assistants imprisoned or persecuted for doing their job, exposes mistreatment and torture, fights censorship, financial aid to journalists and their families.	Reporters sans frontières 47 rue vivienne 75002 Paris – France	www.rsf.org
Scholars at Risk	Scholars at Risk is an international network of institutions and individuals working to promote academic freedom and to defend the human rights of scholars worldwide	Scholars at Risk Network, c/o New York University, 194 Mercer St, New York, New York 10012, USA	http://scholarsatrisk.nyu.edu

Organisation	What They Do	Address	Website
South Asia Forum for Human Rights (SAFHR)	Provides human rights NGOs and activists an opportunity to expose abuses. Organises regional dialogues, produces research and publications and undertakes advocacy campaigns.	See website	http://www.safhr.org/
Southeast Asia Press Alliance (SEAPA)	Works on freedom of expression in South East Asia, including urgent alerts.	No.115 Thakolsuk Place Unit 3B Terddamri Rd. Dusit 10300 Bangkok, Thailand	http://www.seapabkk.org/
UN Special Rapporteur on the situation of human rights defenders	Protection of defenders themselves and the protection of their right to defend human rights. Includes visits, holding workshops and producing publications.	Office of the United Nations High Commissioner for Human Rights (OHCHR) Palais Wilson 52 rue des Pâquis CH-1201 Geneva, Switzerland	http://www2.ohchr.org/english/issues/defenders/index.htm
The Rory Peck Trust	Supports freelance newsgatherers and their families. Subsidises training in hostile environments, provides direct practical support to freelancers in need, and to the families of those killed during their work.	The Rory Peck Trust 2 Grosvenor Gardens, London SW1W 0DH, UK	http://www.rorypecktrust.org/
South Caucasian Network for Human Rights Defenders	The Network seeks to facilitate creation of a safer and enabling environment for human rights defenders in the South Caucasus and to strengthen their voices in the region and internationally.	See website	http://www.caucasusnetwork.org/
USAID	Financial assistance for expanding democracy while improving the lives of the citizens of the developing world.	Information Center U.S. Agency for International Development Ronald Reagan Building Washington, D.C. 20523-1000	http://www.usaid.gov
WOMEN			
Arab Women's Fund (MENA)	Provides support and funding for women's organizations that work toward women's rights in the MENA region.	See website	http://www.arabwomensfund.org/
Asia-Pacific Forum on Women, Law and Development (APWLD)	APWLD empowers women in the region to use law as an instrument of change for equality, justice, peace and development. APWLD uses research, training, advocacy and activism to strengthen women's human rights.	See website	http://www.apwld.org/
AWID (Association for Women's Rights in Development)	Strategic initiatives to advance women's rights and gender equality worldwide.	See website for offices	http://www.awid.org/
Global Fund For Women	Advocate for and defend women's human rights by making grants to support women's groups around the world.	Global Fund for Women 222 Sutter Street, Suite 500, San Francisco, CA 94108, USA	http://www.globalfundforwomen.org
International Women's Rights Watch and International Women's Rights Watch Asia Pacific (IWRAW-AP)	IWRAW focuses on building and supporting capacity – both among NGOs and within the treaty bodies – for using the entire international treaty system as a key to accountability for women's human rights.	See websites	http://www1.umn.edu/humanrts/iwraw/index.html and http://www.iwraw-ap.org/
JASS (working in Mesoamerica, Southern Africa and Southeast Asia)	Seeks to build women's political influence, ensure their access to resources, and protect their safety as activists.	See website	http://www.justassociates.org/

Organisation	What They Do	Address	Website
Women Human Rights Defenders International Coalition	Resource and advocacy network for the protection of women human rights defenders	See website	http://www.defendingwomen-defendingrights.org/
Urgent Action Fund for Women's Human Rights	Urgent Action Fund for Women's Human Rights (UAF) is a global women's fund that exists to protect, strengthen and sustain women human rights defenders at critical moments in time.	3100 Arapahoe Ave., Suite 201, Boulder, Colorado 80303 USA	http://www.urgentactionfund.org/index.php?id=51
Urgent Action Fund – Africa	UAF-Africa links the activities of women with the resources they require to respond to conflict and to take advantage of opportunities to advance women's human rights.	Urgent Action Fund-Africa, CVS Plaza, 2nd Floor, Lenana Road, Kilimani, P.O. Box 53841-00200, Nairobi. Kenya.	www.urgentactionfund-africa.or.ke
Women Living Under Muslim Laws	International solidarity network for women whose lives are shaped or governed by laws and customs said to derive from Islam. Aims to strengthen women's individual and collective struggles for equality and their rights, especially in Muslim contexts.	Several offices – see website	http://www.wluml.org
LGBTI			
ARC International	Facilitating strategic planning around LGBT issues internationally, strengthening global networks, and enhancing access to UN mechanisms. Strengthening capacity of LGBTI.	See website	http://www.arc-international.net
ASTRAEA	Astraea provides financial support to lesbian-led, trans, LGBTI and progressive organizations.	Astraea Lesbian Foundation For Justice 116 East 16th Street, 7th Floor, New York, NY 10003	www.astraeafoundation.org
Coalition of African Lesbians	Work to transform Africa into a place where all lesbians enjoy the full range of human rights	See website	http://cal.org.za/
International Gay and Lesbian Human Rights Commission (IGLHRC)	Building partnerships with NGOs globally, advocating for the elimination of discriminatory laws, policies and practices, supporting anti-discrimination laws policies and practices.	IGLHRC 80 Maiden Lane, Suite 1505, New York, NY 10038	http://www.iglhrc.org
International Lesbian, Gay, Bisexual, Trans and Intersex Association (ILGA). Europe	Represents its members, principally organisations of lesbian, gay, bisexual and transgender persons, at the European level.	ILGA-Europe rue Belliard straat 12 Brussels B-1040 Belgium	http://www.ilga-europe.org/
Fellowships & Scholarships			
York Fellowship	York University Protective Fellowship for HRDs to spend time away from difficult environments whilst benefiting from educational resources designed to increase their effectiveness and their ability to influence policy and practice at home.	Centre for Applied Human Rights , University of York, Heslington, York, UK. YO10 5DD	http://www.york.ac.uk/inst/cahr/defenders/index.html
Oak Fellowship	The Oak Fellowship offers an opportunity for one prominent practitioner in international human rights to take a sabbatical leave from the front-line. This provides the Fellow with time for respite, reflection, research, and writing.	4000 Mayflower Hill, Waterville, ME 04901	http://www.colby.edu/academics_cs/goldfarb/oak/
Scholar Rescue Fund Fellowships	The Scholar Rescue Fund provides fellowships that give temporary refuge at universities and colleges anywhere in the world for established scholars whose lives and work are threatened in their home countries.	Scholar Rescue Fund Institute of International Education 809 United Nations Plaza New York, New York 10017-3580 USA	http://www.scholarrescuefund.org/pages/about-us.php

Organisation	What They Do	Address	Website
Taiwan Foundation for Democracy Fellowship	International Visiting Fellowships, for experienced democracy and human rights practitioners, plus other fellowships.	No.4, Alley 17, Lane 147, Sec. 3, Sinyi Rd., Taipei 106, Taiwan	http://www.tfd.org.tw/english/fellowships.php
Hamburg Foundation for the Politically Persecuted	The Foundation works with HRD organizations providing grants and scholarships to politically persecuted people. It also initiates and supports petition campaigns for political prisoners and missing persons.	Hamburger Stiftung für politisch Verfolgte Osterbekstraße 96, 22083 Hamburg	http://www.hamburger-stiftung.de/e_index.html
Reagan-Fascell Democracy Fellows Program at the National Endowment for Democracy	This Fellows Program enables democracy activists, practitioners, scholars, and journalists from around the world to deepen their understanding of democracy and enhance their ability to promote democratic change.	National Endowment for Democracy 1025 F Street NW, Suite 800 Washington, DC 20004	http://www.ned.org/fellowships
International Cities of Refuge Network (ICORN)	ICORN provides writers with a safe place to stay and economic security for a standard term of two years, ICORN promotes Freedom of Expression one writer at a time.	Sølvberget KF, Stavanger Cultural Centre P.O. Box: 310, 4002 Stavanger, Norway	http://www.icorn.org/
Prizes for Human Rights Defenders			
Asia Democracy and Human Rights Award	Awarded by the Taiwan Foundation for Democracy for an individual or organization which has made major contributions through peaceful means to the development of democracy and human rights in Asia	No.4, Alley 17, Lane 147, Sec. 3, Sinyi Rd., Taipei 106, Taiwan	http://www.tfd.org.tw/english/HTML/ADHRA0408.html
Front Line Award	The Front Line Award for Human Rights Defenders at Risk, was established to highlight the work of outstanding individuals who on a daily basis put their security and lives at risk defending the human rights of others.	Front Line - The International Foundation for the Protection of Human Rights Defenders Grattan House, 2nd Floor, Temple Rd, Blackrock Co Dublin, Ireland	http://frontlinedefenders.org/front-line-award-human-rights-defenders-risk
Goldman Environmental Prize	The Prize honours grassroots environmentalists.	160 Pacific Avenue, Suite 200, San Francisco, CA 94111, USA See website	http://www.goldmanprize.org/
Gwangju Human Rights Prize (for Asian HRDs)	Human Rights Prize for Asian HRDs	See website	http://eng.518.org/eng/html/main.html
Martin Ennals Award	The award aims at encouraging HRDs who are at risk and in need of immediate protection.	See website	http://www.martinennalsaward.org/
Tulip Award	The Dutch Government's human rights award, the Human Rights Defenders Tulip has since 2008 been presented to an individual who has shown exceptional courage in protecting and promoting the rights of fellow human beings.		http://www.humanrightstulip.org/simplepage/home/
International Women of Courage Award	The US Government's Awards for remarkable women of courage		http://www.state.gov

NOTES

WORKBOOK ON SECURITY:
PRACTICAL STEPS FOR HUMAN RIGHTS DEFENDERS AT RISK

WHAT DOES FRONT LINE DO?

Front Line was founded in Dublin in 2001 with the specific aim of protecting human rights defenders at risk, people who work, non-violently, for any or all of the rights enshrined in the Universal Declaration of Human Rights (UDHR). Front Line aims to address the protection needs identified by defenders themselves.

Front Line seeks to provide rapid and practical support to at-risk human rights defenders, including through:

- international advocacy on behalf of human rights defenders at immediate risk;
- grants to pay for the practical security needs of human rights defenders;
- training and resource materials on security and protection, including digital security;
- rest and respite, including the Front Line Fellowship;
- opportunities for networking and exchange between human rights defenders;
- the annual Front Line Award for Human Rights Defenders at Risk;
- an emergency 24 hour phone line for human rights defenders operating in Arabic, English, French, Spanish and Russian.

Front Line promotes strengthened international and regional measures to protect human rights defenders including through support for the work of the UN Special Rapporteur on the situation of human rights defenders. Front Line seeks to promote respect for the UN Declaration on Human Rights Defenders.

Front Line has Special Consultative Status with the Economic and Social Council of the United Nations. Front Line has Observer Status with the African Commission on Human and Peoples' Rights. Front Line received the 2007 King Baudouin Prize for International Development.

WWW.FRONTLINEDEFENDERS.ORG
PROTECT ONE: EMPOWER A THOUSAND

European Commission

Irish Aid
Department of Foreign Affairs
An Roinn Gnóthaí Eachtracha

978-0-9558170-9-0

Front Line Head Office
Second Floor, Grattan House
Temple Road. Blackrock
Co. Dublin

Tel: 00 353 1 212 37 50
Fax 00 353 1 212 10 01

FRONT LINE DEFENDERS

Front Line – Brussels Office
Square Marie-Louise 72
1000 Brussels,
Belgium

Tel: 00 32 2 230 93 83
euoffice@frontlinedefenders.org