

# A Guide to Personal Security for Human Rights Defenders



**Facilitators' Edition**



Copyright © 2010 by Bridges Across Borders Cambodia. All rights reserved.

*A Guide to Personal Security for Human Rights Defenders  
Facilitators' Edition*

First edition: August 2010

We encourage others to copy, reproduce or adapt to meet local needs any or all parts of this book, provided that the parts reproduced are attributed to the original publication and are distributed not-for-profit. Any organization or person who wishes to copy, reproduce, or adapt any or all parts of this book for commercial purposes must obtain permission from the publishers.

Before beginning any translation or adaptation of this book or its contents, please contact the publishers for suggestions, for updates on the information it contains, and to avoid duplication of efforts. Please send the publishers a copy of any materials in which text from this book has been used.

Bridges Across Borders Cambodia  
#144-H Street 143  
Boeung Keng Kang III, Khan Chamcarmon  
Phnom Penh, Cambodia  
Email: [office@babcbodia.org](mailto:office@babcbodia.org)  
Web: [www.babcbodia.org](http://www.babcbodia.org)

Financial support provided by:



## **ACKNOWLEDGEMENTS**

*A Guide to Personal Security for Human Rights Defenders* was researched, written and field tested through 2009 and 2010. The project was supported by a grant from the Swedish Amnesty Fund, with assistance for production costs provided by the United Nations Office of the High Commissioner for Human Rights. It was implemented by the BABC Community Empowerment and Legal Awareness Program (CELA), which receives funding from the British Embassy in Cambodia, McKnight Foundation, Norwegian People's Aid (NPA), Open Society Institute (OSI), and Planet Wheeler Foundation.

To each of our funding partners, we are deeply thankful for their support, and for enabling this project to become a reality.

### **AUTHOR:**

Mark Grimsditch

### **FIELD-TESTING AND REVIEW TEAM:**

Bun Makara  
Chan Vichet  
Eang Vuthy  
Alexandra Jones  
Ros Sothida  
Sao Sotheary  
Sor Nyphana

### **GENERAL EDITORS:**

Maia Diokno  
Mark Grimsditch  
David Pred  
Sao Sotheary

## ILLUSTRATIONS:

Illustrations for this publication were provided by artists at Our Books  
(<http://www.siewphewyeung.org.kh>)

Soeun Klo (Coordinator)  
Chan Ny  
Moeu Diyadaravuth  
Phal Phourisith  
Tek Tevinn  
Sin Yang Pirom  
Srey Ratanak

Sao Channa (graphic assistance)

## COVER DESIGN:

Chan Vichet

We would also like to acknowledge the following individuals, who contributed, reviewed and provided important guidance and suggestions on the overall approach, content, activities and methodology of this manual: Keat Bophal, Maia Diokno, Eang Vuthy (translation), Alexandra Jones, Tamara Mosher-Kruzer (for initial research), Jocelyn Medallo, Sek Sokha (translation), and Som Sothanin.

Parts of this curriculum were based on existing security curriculum developed for other countries around the world. The concepts contained in Frontline's *Protection Manual for Human Rights Defenders* were especially useful in developing this Cambodia specific guide. To view this manual, visit <http://www.frontlinedefenders.org/en/> (Frontline is not affiliated with this publication).

We would also like to thank the Cambodian human rights defenders who participated in the field-testing workshop conducted in 2010, for their constructive feedback and support.

Finally, this guide could not have been written without the thoughtful feedback from dozens of Cambodian rights activists and community network members who have helped develop and improve the curriculum of the Bridges Across Borders Cambodia Community Empowerment and Legal Awareness Program at every step along the way.

# CONTENTS

<b>HOW TO USE THE GUIDE</b> .....	<b>1</b>
1. ORGANIZING A TRAINING .....	1
2. STARTING A TRAINING .....	3
3. INTERACTIVE TEACHING .....	4
4. TEACHING METHODS.....	5
5. LESSON PLANS .....	11
<b>WHAT DOES SECURITY MEAN TO YOU?</b> .....	<b>15</b>
1. WHAT IS SECURITY?.....	15
<i>LESSON 1: WHAT DOES SECURITY MEAN TO YOU, AND WHY IS IT IMPORTANT?</i> .....	18
2. WHAT SECURITY RISKS DO ACTIVISTS AND HUMAN RIGHTS DEFENDERS FACE?.....	21
<i>LESSON 2: WHAT RISKS DO HUMAN RIGHTS DEFENDERS AND ACTIVISTS FACE?</i> .....	26
<b>IDENTIFYING SECURITY THREATS</b> .....	<b>33</b>
1. IDENTIFYING WHERE SECURITY RISKS COMES FROM .....	33
<i>LESSON 1: IDENTIFYING WHERE SECURITY THREATS CAN COME FROM</i> .....	35
2. PREDICTING AND IDENTIFYING POSSIBLE THREATS .....	38
<i>LESSON 2: PREDICTING AND IDENTIFYING THREATS</i> .....	41
3. ASSESSING THE SERIOUSNESS OF A THREAT.....	45
<i>LESSON 3: ASSESSING THE SERIOUSNESS OF A THREAT</i> .....	49
<b>PRACTICAL SECURITY: MINIMIZING RISKS</b> .....	<b>61</b>
1. MINIMIZING RISKS .....	61
2. PRACTICAL STEPS.....	61
<i>LESSON 1: MINIMIZING SECURITY THREATS</i> .....	66
<b>RESPONDING TO SECURITY THREATS</b> .....	<b>71</b>
1. HOW DO YOU RESPOND TO SECURITY THREATS?.....	71
<i>LESSON 1: HOW DO YOU RESPOND TO SECURITY THREATS?</i> .....	73
2. STRATEGIES FOR RESPONDING TO THREATS .....	76
<i>LESSON 2: HOW DO YOU RESPOND TO SECURITY THREATS?</i> .....	82
3. REPORTING INCIDENTS.....	85
<i>LESSON 3: REPORTING INCIDENTS</i> .....	89

<b>LEGAL THREATS: INCITEMENT, DEFAMATION &amp; FALSIFICATION OF INFORMATION ....</b>	<b>95</b>
1. COMMON LEGAL THREATS TO HUMAN RIGHTS DEFENDERS .....	95
<i>LESSON 1: INCITEMENT, DEFAMATION AND FALSIFICATION OF INFORMATION .....</i>	<i>102</i>
<b>THE LAW ON PEACEFUL DEMONSTRATION .....</b>	<b>111</b>
1. WHAT IS A DEMONSTRATION? .....	111
2. WHAT DOES THE LAW SAY ABOUT DEMONSTRATIONS? .....	112
<i>LESSON 1: THE LAW ON PEACEFUL DEMONSTRATION .....</i>	<i>115</i>
3. STAYING SAFE AT DEMONSTRATIONS.....	120
<i>LESSON 2: STAYING SAFE AT DEMONSTRATIONS .....</i>	<i>122</i>
<b>YOUR RIGHTS AFTER ARREST .....</b>	<b>127</b>
1. ARREST.....	127
2. RIGHTS IMMEDIATELY AFTER ARREST .....	127
<i>LESSON 1: YOUR RIGHTS IMMEDIATELY AFTER ARREST .....</i>	<i>131</i>
3. WHAT CAN YOU DO IF A FRIEND, FAMILY MEMBER OR COLLEAGUE IS ARRESTED? ....	134
<i>LESSON 2: WHAT CAN YOU DO IF SOMEONE IS ARRESTED OR DETAINED?.....</i>	<i>137</i>
<b>ANNEX 1: FACTSHEET – INFORMATION SECURITY .....</b>	<b>143</b>
<b>ANNEX 2: FACTSHEET – WORKING WITH A LAWYER .....</b>	<b>147</b>
<b>ANNEX 3: CONTACT LIST .....</b>	<b>149</b>

# INTRODUCTION

Across the world, human rights defenders routinely face intimidation, threats, false prosecution and deprivation of liberty, and, in some cases, violent attack or even murder. Powerful actors routinely use these strategies to break movements and spread fear amongst activists. The work of human rights defenders is vital, and it is because of this work that many of us enjoy the freedoms that we do today.

In many places, community activists and networks are on the frontline of the human rights struggle, and because of this, are frequently exposed to significant security risks. Sometimes these risks are unavoidable; other times they are the result of a lack of awareness or adequate planning. With this in mind, BABC has researched and developed this guide in collaboration with its partners and with prominent Cambodian community activists.

The guide covers basic practical tips for improving personal security, including how to identify risks, how to minimize them and how to react, in the event that a threat becomes real. This material is intended as a starting point, and this basic training course provides a foundation for more detailed and thorough security planning.

The guide uses interactive activities to help people understand the information, take part in discussions, and learn important skills, even if they cannot read or write. This way, everyone can participate in planning what they can do to defend their rights and the rights of fellow citizens.



# HOW TO USE THE GUIDE

*A Guide to Personal Security for Human Rights Defenders* has been designed and written so that it is accessible to communities, including those who have had limited access to education and have little or no knowledge of the subjects. The language used is simple and straightforward and the exercises used are interactive and enjoyable. Everything in this manual has been tried and tested with communities around Cambodia and the authors have considered all feedback and comments in revising and finalizing the lessons.

The guide can be used by people who want to facilitate a training workshop and by people who would like to use it simply as an information resource. The guide is made up of the Facilitators' Edition and the Participants' Edition. The Facilitators' Edition includes all the instructions and everything else you need to run a training session. The Participants' Edition contains only the information on each topic without the facilitator's instructions. It is useful to provide copies of the Participants' Edition to the people who attend your training. It can also be used by human rights defenders as a stand-alone resource.

This module explains the basics on how to use the guide and how to organize and deliver a community training.

## 1. ORGANIZING A TRAINING

First, you will need to organize the training workshop. It is important that everything – from the venue, to the selection of modules you will be teaching – is prepared well in advance, and that you are organized. If things do not run smoothly, the training will not be as effective. When organizing a training workshop you should consider the following points:

### 1.1. BOOKING A VENUE

It may be possible to teach in the community, or you may need to find or hire a room to hold the training. Make sure the venue is quiet and bright and has enough space for all the participants to work comfortably. Make sure that you have decided on and booked the venue at least two weeks before the training.

### 1.2. PARTICIPANTS

You will need to decide who should participate in the training. It may be people from one or more communities threatened with eviction, members of a community network or people from NGOs. You may even decide to teach government officials or company employees. Think about who will benefit from the training. You should also consider

who will be able to attend and stay for the whole training. Think about how many people should participate – usually an ideal number of participants is between 15 and 25.

Try to make sure that you have a good mix of participants. There should be equal numbers of men and women, and sometimes it is a good idea to have mixed age groups, as people have different experiences to share. If you are training in an area that has a number of ethnic groups, for example Cham or indigenous minorities, it is important to involve people from these groups in the training and ensure that everyone is treated equally.

### **1.3. NOTIFICATION AND INVITATIONS**

Make sure you inform all participants about the training dates well in advance. When the date gets closer, send reminders.

### **1.4. PARTICIPANTS' SITUATIONS**

Try to find out what specific problems the participants are experiencing and what their stories are. This way you can decide which sections of the guide are most important to teach. It is also a good idea to ask a few community representatives what topics they think would be most useful.

### **1.5. AGENDA**

Once you have the information about the participants you will need to prepare an agenda. This sets out the plan for each day of the workshop. Make sure you have enough time to teach the lessons you have selected. Make sure you also include time for breaks, meals and energizers (explained below).

### **1.6. INFORMING AUTHORITIES**

Think carefully about whether it is necessary to inform the local authorities of your plan to conduct a community training.

### **1.7. PARTICIPANT'S GUIDE**

At the end of the training it is a good idea to provide the participants with all the information that you have covered. To do this, you will need to photocopy the relevant sections of the Participants' Edition.

## 1.8. BE PREPARED

Make sure you are familiar with the material that you will teach, and make sure that before the workshop starts, you have all the materials that are necessary for each lesson. If there are other facilitators, make sure you have decided who will be responsible for each lesson and activity.

### TRAINING CHECKLIST

Before conducting a training, make sure that you do the following:

Organize a venue

Decide who the Participants will be and how many will attend

Invite the Participants well in advance, and send a reminder closer to the date

Learn about the Participants' background, situation and which topics they are interested in

Choose the modules you will teach and make an agenda

Inform the authorities, if you think it is necessary

Photocopy relevant parts of the Participant's Guide

Prepare the materials, for example, paper, pens and handouts

Revise the lessons so you feel confident to teach them

## 2. STARTING A TRAINING

On the day of the training arrive at the training space or room early to make sure everything is ready. Arrange the materials neatly so that you can access them easily when you need them during the lessons. If tables and chairs are available think about how you would like them to be arranged. Sometimes it is a good idea to arrange the tables in a circle so that everyone can see each other and no one has to sit behind someone else. This will help the training be more interactive because everyone will feel included.

Once the participants arrive and sit down, the first step is to introduce yourself to the group and give participants the chance to introduce themselves. This is done at the beginning of almost all trainings and workshops. In order to start the training in an interesting way, try to keep the introductions short, or try to make them into a game or fun activity. This can be very simple such as asking everyone to say their names, where they are from and their favorite food or song.



It is also a good idea to start the training by explaining the main objectives of the workshop to the participants. You may also want to explain the rules of the training, for example, everyone should turn off mobile phones, everyone should be considerate of other people, there should be no discrimination, and everyone should have a chance to speak. You can also ask the participants about their expectations for the workshop. You may ask a few or all participants to name one thing they expect or hope to learn during the training. You can come back to these expectations at the end of the training to see if they were met.

### **3. INTERACTIVE TEACHING**

The most effective methods for teaching any information are interactive, based on active participation, and focus on the participants, rather than the facilitator. These techniques help people to learn faster and remember more than if they are taught using traditional methods, like lecture.

There have been many studies and experiments that have shown that the amount and quality of the information that participants remember depends on the teaching methods used. Research has shown that the lecture style of teaching is less effective for passing on knowledge to participants. Examples of interactive methodology include:

- Role-play
- Demonstrations
- Stories
- Group discussions

One of the best ways for you to improve your understanding of new information and skills is to teach it to others. By teaching others, you will gain a better understanding, know how to explain things using simple language and be able to show how the information and skills can be used. Community trainings are a two-way learning process. As you teach, the participants learn, and you will also become more confident and increase your understanding of the issues you are teaching. You will also have a valuable opportunity to learn from the experiences and stories of the participants.

## 4. TEACHING METHODS

There are many different teaching methods that can be useful for teaching in communities. These methods are aimed at making those attending the workshop *active participants* and not passive observers. These methods recognize that participants always come to training workshops with knowledge and experience from their own lives and that they have much to contribute to the learning that will happen in the room. Below are some examples of interactive teaching methods.

### 4.1. BRAINSTORMING

Brainstorming is a way of allowing participants to think freely about ideas. There are usually no right or wrong answers, and participants are able to express their ideas freely.

During brainstorming on a particular topic, participants might be asked questions, for example, “What are the different ways to teach?” participants then think of as many different ideas as they can, and these should be written or drawn on a whiteboard or flipchart. Everyone’s ideas can then be discussed.



## 4.2. SMALL GROUP DISCUSSIONS

Small group discussions should be planned carefully. The participants should be given clear rules and instructions and should be allowed enough time for discussion. If possible, the groups should usually not have more than five participants so that everyone has a chance to speak.

## 4.3. CASE STUDIES

Case studies are stories or a description of an event that can be real or made-up and can be used to help understand how information and skills can be applied. Case studies can be used during group discussions to help participants analyze and think critically about how to use new information and skills in practice.



#### 4.4. ROLE-PLAYS

In role-plays participants (or sometimes facilitators) act out a situation. Participants can either be given the situation through a case study or they can be asked to make it up themselves. Different objects that can be found around the training area can be used to make role-plays more fun. Role-plays are useful because participants are able to be creative, which will make them feel more involved in the lesson, and keep them active and interested.

#### 4.5. QUESTION AND ANSWER

A discussion through questions and answers can often be used instead of lecturing. This way everyone is talking and needs to think carefully about the issues, not just the facilitator. Participants almost always know some information about the issue or the subject that is being taught and how it relates to their lives. Good facilitators will draw out the knowledge and experience of participants and build on it. Asking polite questions to quiet participants can be a good way to encourage them to speak and get more involved.

A good way to start teaching a new topic is by asking the whole group some basic questions on the subject. This way you will find out what everybody already knows. Asking questions at the end of the lesson is also a good way to check that participants understood and that the learning objectives were achieved.



## 4.6. GAMES

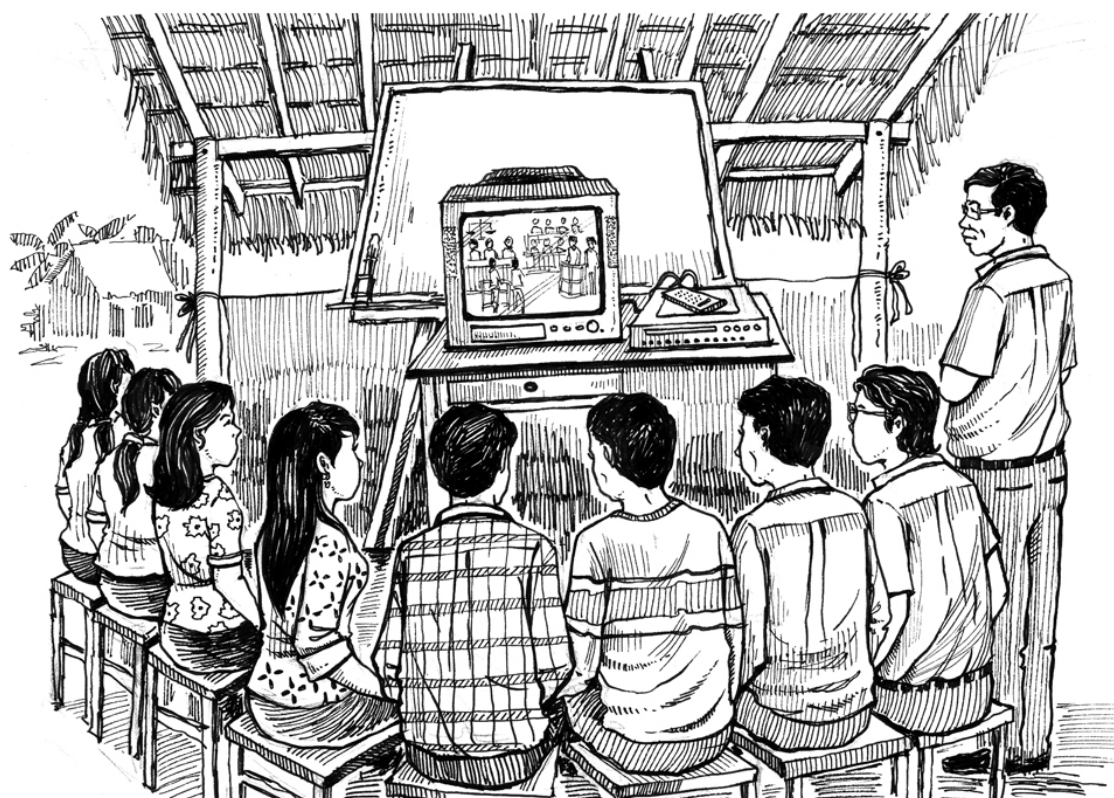
Games are a fun way for both adults and children to learn. Games may be used as ‘ice breakers’ that are fun activities you may use to help participants to get to know each other and become more comfortable with each other. Games are also often used as ‘energizers’ to refresh people when they are feeling unfocused or sleepy between lessons. Games can also be used to teach more difficult topics, such as the law, and to help people remember new information. Games might involve teams and competitions but be careful not to embarrass anyone if they do not know the answers to questions. It can be more encouraging if everyone wins!

## 4.7. PARTICIPANT PRESENTATIONS

Participants can be given a topic, case study or question to work on in small groups and then present to the rest of the class. Groups can be asked to prepare and present drawings, songs, role-plays, plans, ideas, or answers to questions. Presentations can be made by the whole group, or a group spokesperson can be chosen to present. Afterwards, all the participants (both presenters and observers) can discuss the presentation.

## 4.8. VISUAL AIDS

Objects, photographs, pictures, drawings, posters and films are all examples of visual aids. Visual aids help focus participants' attention and are an effective way to bring real life experiences from Cambodia and around the world into the training room. Visual aids are also helpful in expressing ideas, concepts and plans. Participants can be asked to describe and analyze what they see, and apply or compare it to their own experiences and other situations. Visual aids such as films can be especially useful in demonstrating how new skills can be applied. Good and bad examples can be shown and analyzed. (Remember that the same thing can be done using role-plays.)



Many community groups, NGOs and United Nations agencies have produced videos on legal and human rights issues in Cambodia. If you have access to electricity and equipment you can contact these groups and ask if they have any videos you can use in your community training.

## 4.9. SONGS

Most Cambodian people love to sing and dance. You can use this in your training workshops. Sometimes you may want to have a break from the lessons and have a song or dance session just to wake people up. You may also use song to teach. After teaching a topic, you could ask participants to make up a song about it. If this can be done using a popular tune it will make it easy for people to remember the things they learned.



### PARTICIPANTS WITH READING DIFFICULTIES

Sometimes there will be participants in your training workshop that have difficulties reading and writing. You need to be aware of this, although it is not a good idea to ask participants in front of everyone else if they can read and write because this could embarrass them.

Many of the exercises involve case studies and other methods that require some reading and writing. If there are participants who will find this difficult, there are a few things you can do. One option is to make sure there is one member of each group who can read and write so that they can read out case studies or questions and write down ideas or answers for the rest of the group if necessary. If there are not enough Participants who can read, you or another facilitator can read out case studies and help groups to record their answers. You can also think of other ways that groups can record ideas and answers such as through drawings or simply by remembering them.

All activities in this guide can be easily adapted in this way so that all participants, including those with reading difficulties can be actively involved.

## 5. LESSON PLANS

*A lesson plan is like a road map.* If we want to travel somewhere, but are not certain of the correct route, we can use a map. We will look for the start point and our destination, but also the points we need to pass along the way. A lesson plan works in a similar way. The start point is the aim of the lesson, and the final destination is achieving that aim. But to get to this destination, there are steps that you must take to get there.

The lesson plan used in the guide has eight parts. First is the **learning text**, then the **lesson** which is broken into seven smaller parts. These are: the aim, materials, methods used, procedure/time box, instructions to facilitators, suggested answers, and debrief. Below is a brief explanation of the purpose of each of these sections.

### 5.1. LEARNING TEXT

The learning text contains the information about the topic that is being taught. For example, if the lesson is about human rights, the text will include information about what human rights are, where they come from and give some examples of different human rights. Usually the text will also include pictures about the information. The learning text is followed by the exercise instructions.

### 5.2. LESSON

#### 5.2.1. AIM

The Aim is what the participants should learn or understand by doing the lesson.

Example:

**AIM:** Participants will think about what human rights are, where they come from and why it is important to know about them.

#### 5.2.2. MATERIALS

This is a list of things that are needed to teach the lesson. You should make sure that you have all of the items ready before starting the lesson.

Example:

**MATERIALS:** Flipchart or whiteboard, markers, ball, copies of Handout 1.

### 5.2.3. METHODS USED

This is a list of all the interactive teaching techniques used in the lesson.

Example:

**METHOD(S) USED:** Brainstorming, large group discussion, drawing.

### 5.2.4. PROCEDURE/TIME BOX

The left column of this box contains a list of the procedures you should follow to run the lesson. The right column of the table indicates the amount of time required for each step. The total time needed to complete the whole lesson is shown at the bottom. This box is very useful for preparing the workshop agenda.

Example:

Procedure	Time Frame (in minutes)
1. Brainstorm and group discussion	15
2. Introduce the information in Sections 1 & 2	20
3. Small group work	15
4. Group presentations	20
5. Debrief	10
<b>Total:</b>	<b>80</b>

### 5.2.5. INSTRUCTIONS TO FACILITATORS

This part of the manual explains in detail how to carry out all the stages of the lesson, as set out in the procedure table. It includes tips and advice that will help you to deliver the lesson effectively.

### 5.2.6. SUGGESTED ANSWERS

If there are questions in the lesson that ask for information rather than opinions, suggested answers will be included.

### 5.2.7. DEBRIEF

The goal of this section is to evaluate whether the Aim of the lesson was achieved. It is very important that you do not simply summarize the information contained in the lesson, as this will not allow you to check whether or not the participants learned the main points. You can check whether the Aim was achieved by using activities such as questions and answers, by asking participants to summarize the lesson, or by using fun games such as quizzes.



# WHAT DOES SECURITY MEAN TO YOU?

## OUTCOMES

After completion of this module, participants will:

1. Understand the meaning of personal security and why it is important.
2. Be aware of common security risks faced by human rights defenders, activists and other people who speak out in defense of human rights.

## 1. WHAT IS SECURITY?

There are many answers to this question, but basically **security** means being safe and free from threats. This can mean safety and protection from danger, from loss or destruction of property, from crime, or from physical harm. It could also mean safety or protection from losing housing, your source of livelihood, employment or access to food. Security can include being protected from other people accessing your private information. Security also means that you *feel* secure. If you feel more secure mentally, you will feel more confident to deal with issues as they come up.

In this manual we will look at the security issues that affect **human rights defenders** and **activists** in Cambodia. Human rights defenders act to defend human rights, either as a group or as individuals. There have been many cases around the world in which activists face security problems because of their defense of human rights. This is because the people or groups who are behind the human rights violations often do not want people to challenge their actions. Unfortunately, to stop people from challenging them, these people or groups sometimes threaten the security of activists.

No training or planning can make you *totally safe*, but here we will look at the possible threats you may face, and ways that you can try to *reduce* those risks. Some of the information that you read or discuss here may be frightening, but if you are aware of potential threats, it is much more likely that you will be able to *reduce* the risk.

In the following lessons we will look at different kinds of security. In this manual, security is broken down into three main areas: physical security, property security and information security. Very often these areas may overlap. Later in the manual we will also discuss the threat of legal charges, as sometimes people can have their security threatened by being charged with committing a criminal offense.

## 1.1. PHYSICAL SECURITY

**Physical security** means being safe from physical attacks. A physical attack is when someone tries to hurt or even kill someone else. This can also include sexual assault.

## 1.2. PROPERTY SECURITY

**Property security** means that your property is safe from being damaged or taken away from you. For example, your home, farmland, and workplace should all be safe from people entering without your permission. Your money, motorbike, and any other possessions should be safe from being stolen or destroyed.

## 1.3. INFORMATION SECURITY

**Information security** means that your personal information is safe and only available to people who you choose. It is important that your personal documents are safe from getting lost, stolen or destroyed. For example, documents like family books, living books, birth certificates, ID cards, and school certificates should all be kept in a safe place. If you lose important documents, you may have problems later.

Some information is also very sensitive. Sometimes activists want to keep information about any activities they do that are related to their activism **confidential** or private. If someone wants to share private information with others, this is their choice, but they must be very careful if this is likely to effect other people. For example, members of a community network have a duty to keep information related to network activities safe.



## WHY IS SECURITY AWARENESS IMPORTANT?

If you lock the door when you go to sleep at night, you are actively making yourself and your property more secure. If you know that you are taking steps to prevent or reduce security threats, you will feel safer, more comfortable and more confident to continue your work – and hopefully you will *actually be safer*. Sometimes people try not to worry about the problems or threats they face. Ignoring a problem may make you *feel* more secure, but this is not real security. In the following lessons, we will look at how to think about the security threats or problems you may face, and ways that you can try to avoid these problems, or at least reduce the risks.

In addition to the types of security we discussed above, it is also important to think about the security of your organization, network, community or group. As you study the following lessons, try to think not just about your own security, but the security of you family, friends, colleagues, and partners. Think about how you can act together to make each other safer.

## LESSON 1: WHAT DOES SECURITY MEAN TO YOU, AND WHY IS IT IMPORTANT?

**AIM:** Participants will share their understanding of the term "security" and talk about why it is important to them that they are secure in their work and their lives.



**MATERIALS:** Whiteboard/flipchart, markers, small sheets of paper

**METHOD(S) USED:** Whole group discussion, brainstorming.

Procedure	Time Frame (in minutes)
1. Silent brainstorm	5
2. Whole group discussion	20
3. Introduce information from Section 1	20
4. Debrief	15
<b>Total:</b>	<b>60</b>

## INSTRUCTIONS TO FACILITATOR

### 1. SILENT BRAINSTORM:

- To start the lesson, ask all the participants to close their eyes for one minute and think about what the word "security" means to them.
- After one minute, give each participant a small piece of paper and ask them to write a short explanation or draw a picture of what they think of when they think about the word "security". Explain that there is no right or wrong answer, and that they should write or draw whatever they want to.
- Give the participants a few minutes to finish and then give everyone some tape and ask them to stick the papers up on the wall or whiteboard.

### 2. WHOLE GROUP DISCUSSION:

- For the next 20 minutes, facilitate a group discussion on what the participants think security means to them. Use the ideas that participants thought of during the silent brainstorm session.
- To do this, look at the papers on the wall and choose an interesting example. Ask who it belongs to and ask him/her to explain his/her answer. Open the discussion to the rest of the class and ask if anyone else would like to comment.
- Choose another paper and do the same again.
- Ask some volunteers why they think security is important to them. This can be in their daily lives as well as in their work as activists.
- Explain that in the following lessons they will look more at specific security threats and what they can do to try and reduce them.

### 3. INTRODUCE INFORMATION FROM SECTION 1:

- After the discussion, introduce the information from Section 1.

**Section 1** - It is important that participants understand:

- The meaning of security.
- The different types of security.
- Why security is important.

#### 4. DEBRIEF:

- After you have introduced the information from Section 1, write on the board or flipchart: physical security, property security and information security.
- Look again at the papers that were stuck on the wall earlier. Ask participants to think about the three types of security discussed earlier, and then look at the different answers and drawings.
- Ask participants if they can identify which type of security the drawings are about.
- For example, someone may have said earlier: "Security is being safe from having your things stolen or damaged": this is property security. Someone else may have said "Security is being safe from other people harming you or your family": this is physical security. (Some examples may cross over and come under more than one group also.)
- Explain that during the following training, we will talk more about different kinds of security, how to identify threats, and practical steps for minimizing risks and responding to threats.

## 2. WHAT SECURITY RISKS DO ACTIVISTS AND HUMAN RIGHTS DEFENDERS FACE?

### 2.1. KNOWING THE RISKS

All around the world, human rights defenders and activists are working to end rights violations, and to pressure their governments to respect and protect human rights. It is because of the work of these people that many of us enjoy the freedoms that we do today. However, human rights defenders and activists still face many problems.

Sometimes these people may come into conflict with powerful people, companies and institutions. This can lead to intimidation and threats to their safety or freedom. These threats may come from security forces, authorities, individuals or company staff. In some cases it may be unclear where the threats come from.

Often, threats and intimidation do not develop into actual harm. The threat itself might be enough to scare people into stopping their activism. However, there are cases when threats are carried out and people are harmed, imprisoned or, in some cases, even killed. In this section we will look at some of the main threats that activists from all over the world face.

#### THE IMPORTANCE OF KNOWING THE RISKS

Some of the information below may be frightening, but it is important to be aware of what the risks are in order to *reduce* the likelihood that they will happen.

In many cases these risks may be small, and every situation is different, but it is important that you are aware. If you are aware of the risks and you develop ways to deal with them, you are more likely to be able to reduce the chances of harm coming to you or your group.

Next we will discuss some specific types of threat. The examples are divided into the three types of security mentioned earlier, *physical* security, *property* security and *information* security. It is important to remember that all situations are different, and the list below discusses very briefly some of the most common threats. Some may not be relevant to you, and you may also face others that are not listed below.

### 2.2. THREATS TO PHYSICAL SECURITY

1. *Obstruction* – Human rights defenders and activists sometimes face **obstruction**, which prevents them from moving around, going about their daily lives or doing their work as activists. For example, authorities may prevent you from travelling, or company workers may prevent you from taking pictures of their work. Sometimes groups are not allowed to hold meetings or workshops. In 2008,

when community activists from around the country tried to bring petitions to Phnom Penh, security forces in some provinces stopped them from travelling.



2. *Threats of violence* – In some cases, you may face threats to your body or your property. Sometimes people may also threaten the safety of your family or friends. A number of activists in Cambodia report that they have been warned to stop their activism or they may be involved in traffic accidents.
3. *Intimidation* – Threats are often used to intimidate people. **Intimidation** is when someone uses fear to try to influence someone else's behavior. For example, someone may tell you that if you talk about a sensitive topic, your family may get hurt. There may be no actual physical harm caused, but the threat may still be just as effective.
4. *Physical violence* – There are cases of activists being threatened with violence. Occasionally these threats are carried out, and there are recorded incidents of security forces or company employees beating people, usually men. Attacks can be on one person, or a group of people.

In extreme cases, some community activists have been threatened with death, and in very rare circumstances have actually been killed. For example, in Phnom Penh in February of 2007, a union leader received telephone death threats warning him to quit his job. He was later shot dead by two men on a motorcycle on his journey to work.

5. *Sexual harassment and assault* – There are many documented cases around the world of **sexual harassment** or **sexual assault** being used against human rights defenders in order to intimidate them. The victims of this type of violation are usually women.
6. *Arbitrary arrest and detention* – All around the world it is quite common for security forces to detain activists in order to disrupt their work. They may be formally arrested or just held without any charge. Sometimes this can be for only a few hours, in other cases it may be for a longer period of time. If someone is arrested or detained without a clear legal reason, this is called **arbitrary arrest** or **arbitrary detention**. According to international and Cambodian law, everyone should be free from arbitrary detention. The law on arrest and detention will be discussed later.
7. *Criminal charges* – A common risk faced by human rights defenders or activists is that they will face criminal charges. In Cambodia, some activists have been charged with trespassing, criminal damage, **defamation**, **incitement** or **disinformation**, even if there is little or no evidence against them. In some cases, strong activists have been found guilty and sentenced to time in jail. This is covered in more detail in the module covering Legal Threats.

### 2.3. PROPERTY SECURITY

1. *Confiscation or destruction of property* – In some cases, **activists have had cameras taken away** from them and confiscated or destroyed. Others have reported having their motorbikes confiscated. This type of action aims to disrupt the work of activists. In some cases, activists have had important documents like petitions confiscated.

### 2.4. INFORMATION SECURITY

There are important security issues concerning your personal and private information. As an activist, you should know what information to keep safe and how to try to keep information confidential.

It is important that any private information that you speak, hear, write or email stays private. For example, a private conversation should not be discussed with or reported in the media. Also, the discussions and documents of your association, organization, network or group should be safe from theft or from being passed to people who should not have access to them.

Information security is also discussed in more detail in *Annex 1: Information Security*.

1. *Informants* – An **informant** is someone who gives private information to someone else. In some cases, an informant may become part of a group or organization in order to monitor them and gather private information. The informant may then give this information to another party who is in conflict with that group. In some cases, a member of your group may be paid to give up private information.
2. *Information theft or loss* – There is the risk that someone could try to steal important information, or that you could lose important information. For this reason, you should keep sensitive information safe, but also try to have back-ups or copies of all information kept in a safe place.
3. *Monitoring emails or phone calls* – In some countries there is technology that can be used to monitor your phone calls and emails. This is called **surveillance**. This can be used by people to find out private and sensitive information.



4. *Tricks and manipulation* – Sometimes you may give away sensitive information without realizing. In some cases you may be tricked or manipulated into doing this. For example, someone that wants to find out about your activities could pretend that they are sympathetic to your situation, or that they support your group. You may start to trust them and give away too much information without realizing that you are putting yourself or your group at risk.

## SECURITY IS YOUR RESPONSIBILITY

States have a responsibility to protect the rights and safety of their citizens. However, in some countries the state is either *not able* to do this well, or in some cases *not willing* to do so.

In this case responsibility often falls on the individual to take extra steps to protect their own security. If you are a member of a group, such as a community network, organization, or a union, you also have a responsibility to your fellow members – and they have a responsibility to you. You have a responsibility to keep private information confidential and a duty to help minimize any security risks that may affect other people in the group.

## LESSON 2: WHAT RISKS DO HUMAN RIGHTS DEFENDERS AND ACTIVISTS FACE?

**AIM:** Participants will be aware of a number of the security risks that human rights defenders and activists face. They will also have an opportunity to share their own stories and experiences.



**MATERIALS:** Whiteboard/flipchart, markers, sheets of paper with different security risks written on them.

**METHOD(S) USED:** Brainstorming, sharing stories, group discussion.

Procedure	Time Frame (in minutes)
1. Introduce information from Section 2.1	10
2. Open discussion	20
3. Introduce information from Section 2.2 – 2.4	30
4. Debrief	20
<b>Total:</b>	<b>80</b>

## INSTRUCTIONS TO FACILITATOR

### 1. INTRODUCE INFORMATION FROM SECTION 2.1:

**Section 2.1** - It is important that participants understand:

- People all around the world experience threats to their security because they work to defend their rights and the rights of others.
- It is important to know what threats you may face in order to be able to minimize risks.

### 2. OPEN DISCUSSION:

- Explain that in the following lesson the group will learn about and discuss specific security threats.
- Before you do that, facilitate a short open discussion where participants can share their own stories and experiences of security threats they have experienced because of their work as activists.
- As different points are raised, you should write them on separate sheets of paper. For example, "Threat of physical violence", or "Threat of arrest". These can be stuck around the room and you can ask a participant to help you if necessary.
- Remember, during this session your job is not to teach. You should facilitate the discussion and help participants to share their stories. If someone makes an interesting point, ask a follow up question to the other participants. For example, "Do you think this is a common problem for activists?" or "Has anyone heard this kind of story before?"

### 3. INTRODUCE INFORMATION FROM SECTION 2.2 - 2.4:

**Section 2.2 - 2.4** : It is important that participants understand:

- Some common threats to physical security.
- Some common threats to property security.
- Some common threats to information security.

- Before the lesson you should prepare a sheet of paper for each of the security risks discussed in this lesson. Write each of the threats clearly on a different piece of paper:

- Obstruction
  - Threat of violence
  - Acts of physical violence
  - Sexual harassment and sexual assault
  - Arbitrary arrest and detention
  - Criminal charges
  - Confiscation or destruction of property
  - Informants
  - Information theft or loss
  - Monitoring of email and phone calls
  - Tricks and manipulation
- Give these out to different participants. Introduce the information from Section 2.2, and as you get to each example, first ask the participant with that sheet of paper to try to explain what he/she thinks it means. You can also brainstorm with the whole group for suggestions.
  - After getting ideas from the participants you can add additional information from the text. For example, when you get to "Obstruction", ask the participant with that paper to try to explain the concept. Then you can add to his/her answer from the text.
  - Remember that some of the information may be frightening to some Participants, so you should be careful as you talk about the different threats. Make sure to explain clearly that the reason that you are discussing these threats is so that people are aware of the possible risks. If people are aware of what could happen, they can act to reduce the risk of it actually happening.
  - As you go through the different threats listed above, if something has already been discussed in the earlier group discussion you do not need to spend too much time on it. If the information has been covered, mention it and move on to the next threat.

#### 4. DEBRIEF:

- To debrief the exercise, participants will look at the different threats discussed during the lesson and think about which of these threats concern them the most.
- Ask the participants with the sheets of paper to come and stand in a line facing the rest of the group. Ask them to hold up the paper so that everyone can see.
- Explain that the rest of the group should rearrange the different participants in the line so that the biggest or most serious concern is on the left, and the lesser concerns closer to the right. For example, if the participants' biggest fear is physical violence, the participant holding this paper should be told to stand on the left. If participants are less concerned about people monitoring their phone calls, this participant should move to the right.
- Explain again that there are no right or wrong answers to this lesson, and all participants may not agree. This is fine, and the aim of the exercise is to encourage discussion, and encourage people to think about identifying key risks.
- Key risks will always be different depending on a number of factors, such as the country, province, place, time, and who is involved in the situation. Assessing risks will be the subject of the next lesson.

## DIFFICULT TERMS:

1. **Activist:** Someone who takes an active part in campaigns, advocacy or other social action.
2. **Arbitrary arrest or detention:** When someone is arrested or detained without a clear legal reason or evidence.
3. **Confidential:** If information is confidential, it is secret and only you can decide who has access to it.
4. **Defamation:** A statement or writing made in bad faith about a person that harms the honor or reputation of that person.
5. **Human rights defenders:** People who act to defend human rights, either as a group or as individuals.
6. **Incitement:** Incitement is when somebody says or writes something that encourages others to break the law.
7. **Informant:** Someone who gives private information to someone else, often for money. Sometimes an informant may join a group to get information, or it may be an existing member of a group who takes money for information from an outsider. Sometimes, if you are tricked into giving away sensitive information, you may become an informant without knowing it.
8. **Information security:** Information security means that your personal information is safe and only available to people who you choose.
9. **Intimidation:** When someone uses fear to try to influence someone else's behavior.
10. **Disinformation:** It is illegal to spread information that you know is untrue, if the information is likely to disturb the peace.
11. **Obstruction:** To make something difficult or impossible. For example, some activists have been stopped from travelling when the authorities know that they are joining an event or action.
12. **Physical security:** Physical security means being safe from a physical attack. A physical attack is when someone tries to hurt or even kill someone. This can also include sexual assault.
13. **Property security:** Property security means that your property is safe from being damaged or taken away from you. For example, your home, farmland, or office should all be safe from people entering without your permission.

14. **Security:** Security means being safe and free from threats. This can mean safety and protection from danger, from loss of property, from crime, or from physical harm.
15. **Sexual assault:** Any assault which has a sexual nature. This may include serious assaults like rape, but can also include touching someone inappropriately without their consent.
16. **Sexual harassment:** Intimidation, pressure or threats which are sexual in nature.
17. **Surveillance:** Being under close observation. If you are under surveillance, someone may listen to your telephone calls, read your emails, and watch where you go and who you meet.



# IDENTIFYING SECURITY THREATS

## OUTCOMES

After completion of this module, participants will:

1. Be able to identify where security risks may come from.
2. Be able to think about ways to predict and identify security risks.
3. Be able to assess the seriousness of a threat.

## 1. IDENTIFYING WHERE SECURITY RISKS COMES FROM

One of the first steps in minimizing security problems is identifying the risks that you face. There are many definitions of what a **risk** is, but one basic definition is: something that might happen in the future and that could cause harm. During this module you will look in more detail at how to identify risks and also how to assess the seriousness of the risk. Later we will discuss ways to reduce the chances of security risks actually happening, or if they do happen, ways to respond to them.

Before you start to look at the specific risks or threats that you may face, it is important to think about *where those risks or threats might come from*.

### 1.1. WHAT INTERESTS ARE INVOLVED?

Threats to security can come from individuals, people inside your group, outsiders, companies, security forces and other authorities. Very often, you may become threatened because your work has an impact on someone else's interests. For example, if you speak out against a development project that you think will harm your community, you are trying to protect your interests, and those of your community. However, you may also impact on the interests of a company, local authorities, and others who hope to benefit from the project.

When identifying where a threat comes from, it is useful for you to think about how the work you do may impact on the *interests* of other people.

- Think about what kind of issues you are working on, what your aims are, who is involved in the work, and who it is likely to have an impact on.
- Think about the interests that you are trying to protect, this may be the right to continue to live on and farm your land, or have access to forest products.

- Think about how other people's interests may be related to your work. This could include a company that hopes to make a lot of money from developing the land that you farm, or it could be a government official or department that has different ideas about the way your area should be developed.
- Think about both possible positive and negative impacts.

In most cases where you are faced with a security threat, there will be more than one individual or group of people involved. Looking at the interests involved may help you to develop a better strategy for dealing with the threat. For example, in some cases there could be involvement of a company, a powerful individual and security forces. If you are planning how to respond to a threat like this you need to consider all the actors who are involved.

For example, a campaign against illegal Economic Land Concessions in 2009 had a lot of support from people across Cambodia, and many signatures were collected for the petition. However, some of those involved in the campaign faced serious security concerns. Although the campaigners ran and organized the action themselves, they had support from many local and international NGOs, who provided practical support, legal advice, and helped the campaigners to make contact with organizations like the UN that could monitor their security situation. However, as the campaign was likely to have an impact on some powerful companies and individuals, a number of people feared that they could face problems for being involved.



Look at this example above and think about what interests may be involved here. What interests are the campaigners trying to protect? Whose interests could be impacted by the campaigner's actions?

## LESSON 1: IDENTIFYING WHERE SECURITY THREATS CAN COME FROM

**AIM:** Participants will be able to think about the different interests that may be involved in the work that they do. They will then use this to consider where different security threats may come from.



**MATERIALS:** Whiteboard/flipchart, markers.

**METHOD(S) USED:** Sharing stories, whole group discussion.

Procedure	Time Frame (in minutes)
1. Introduce information from Section 1	20
2. Participants discuss their own experience of past security threats	20
3. Use one example and look at the different "interests" involved in that case	20
4. Debrief	15
<b>Total:</b>	75

## INSTRUCTIONS TO FACILITATOR

### 1. INTRODUCE INFORMATION FROM SECTION 1:

- Start the lesson by introducing the information from Section 1.

**Section 1** - It is important that participants understand:

- A first step in identifying threats is being able to identify where that threat comes from.
- When looking at where a threat comes from, it is important to think about whose interests are involved.

### 2. PARTICIPANTS DISCUSS THEIR OWN EXPERIENCES OF PAST SECURITY THREATS:

- After introducing the information from Section 1, ask participants to share with the rest of the group some of their own experiences of times when they have experienced threats to their security.
- Make sure that nobody feels pressured into speaking, and only ask those who are comfortable to talk about their experiences.
- Explain that after this short session where participants will share stories, the group will look at one case in more detail and think about what interests were involved in the situation, and how it was resolved.

### 3. USE ONE EXAMPLE AND LOOK AT THE DIFFERENT "INTERESTS" INVOLVED IN THAT CASE:

- After the sharing session, take one interesting example and ask the participant who presented it if you can ask some follow up questions.
- Explain that for the next 20 minutes the whole group will look at this case and think about where that threat came from. Make sure that everyone is involved in the discussion, not just the person who told the story.
- Facilitate a discussion using the following questions:
  - Who was responsible for the actual threat?
  - Who helped you deal with the threat?
  - Who worked against you?

- Who else do you think may have had an interest in this case? Do you think they may be involved in the security threat you faced?
  - Why do you think you/your group was targeted?
  - What was the final result?
- Try and make the discussion as free as possible and less like a question and answer session. The aim is to get the participants to think beyond the actual security threat they are discussing and to think more about where the threat is from and who may be involved.

#### 4. DEBRIEF:

- In this lesson participants looked at how to identify where different security threats might come from, and who may have an interest in the work that they are doing.
- Hopefully they will realize that this is not always a simple task, and will be different for different situations.
- To close the lesson, ask participants to think about the stories that they heard earlier as well as the case they just looked at in more detail. Ask if they see similarities between their stories and also other experiences they have had in the past.
- In the next lesson participants will look in more detail at predicting and identifying threats.

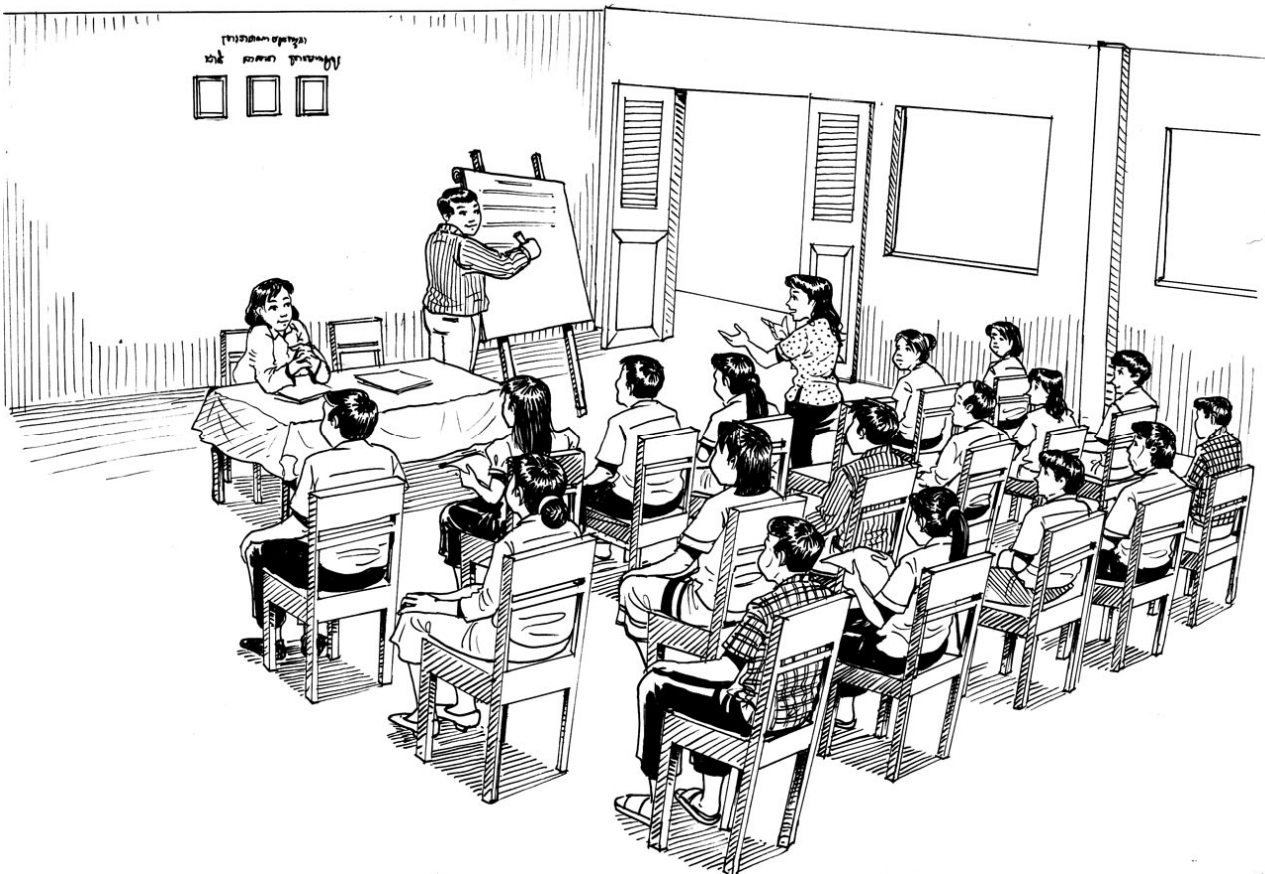
## 2. PREDICTING AND IDENTIFYING POSSIBLE THREATS

Now we have looked at where security threats may come from, and the different actors who may have an impact on your security situation, the next step is to think about what those threats may actually look like.

It is important that you are able to both *predict* threats before they happen as well as being able to *identify* threats as they occur. Of course, predicting a threat is not always easy.

### 2.1. PREDICTING THREATS

The best way to minimize security risks is to be **pro-active**. Being pro-active means that you act *before* something happens. If you identify a threat before it becomes real, you can act to avoid it, or you can at least be prepared. The opposite of being pro-active is being **re-active**. This means that you act *after* the harm has already happened. It is much better to avoid or minimize harm by acting first.



As we already discussed, the first step in assessing your security situation is to look at where threats may come from. Next you can think about what a threat may look like, and what the warning signs or indicators might be. Also think about:

- *What activities* do we have planned? (Some activities are more sensitive than others);

- *What area* are we working in? (In more remote areas you may be less safe, or in border areas or areas with a high military presence);
- *When* are we doing this? (Some periods can be more risky than others to do advocacy or organize activities. For example, around election time, or if there is a period of political or social tension it may be more risky to hold an event.)

## 2.2. MONITORING SECURITY IS NOT A ONE-OFF ACTIVITY

Monitoring your security situation is not something that you can do once and then forget about. For example, if you are organizing an event or some kind of action, it is important to assess the security situation at the early stages of *planning* any activities, *during* the activity and *afterwards*.

For example, a community involved in a land dispute plans to collect thumbprints on a petition and bring the petition to Phnom Penh to give to the National Assembly. They should assess security concerns:

- When they are *planning* this activity: For example, when deciding which community members will collect the thumbprints, how and where they will do this, and who will bring the petition to Phnom Penh.
- *During* the activity: For example, during collection of thumbprints and travelling to Phnom Penh.
- *After* the action is finished: For example, will the organizers receive pressure from the authorities?

## 2.3. IDENTIFYING ACTUAL THREATS

Earlier we talked about the kinds of threats that human rights defenders and activists sometimes face. These can include:

- *Verbal threats*, e.g. someone telling you that you will be physically harmed or arrested.
- *Written threats*, e.g. a letter could be sent by authorities warning that you may be arrested if you continue your advocacy, or someone may write an anonymous note warning you to stop.
- *Symbolic threats*, e.g. one activist reported finding a bullet on his door step, this was a message to him to stop his activities.

- *Implied threats*, e.g. sometimes a threat can be made by something that is not actually said. It can be implied or assumed from someone's behavior or gestures.
- *Physical threats*, e.g. direct violence.
- *Legal threats*, e.g. the threat of arrest or being charged with committing a criminal offence.
- *Social threats*, e.g. sometimes other people are warned against talking to activists or doing business with them.

## LESSON 2: PREDICTING AND IDENTIFYING THREATS

**AIM:** Participants will build on the previous lesson and look at ways to predict possible threats.



**MATERIALS:** Whiteboard/flipchart, markers.

**METHOD(S) USED:** Small group discussions.

Procedure	Time Frame (in minutes)
1. Introduce information from Section 2	20
2. Open discussion	20
3. Explain exercise and divide participants into groups	5
4. Groups identify security threats	20
5. Debrief	15
<b>Total:</b>	<b>70</b>

## INSTRUCTIONS TO FACILITATOR

### 1. INTRODUCE INFORMATION FROM SECTION 2:

- Start the lesson by introducing the information from Section 2.

**Section 2** - It is important that participants understand:

- The need to be pro-active, rather than re-active.
- It is better to predict security threats before they happen.
- Monitoring your security situation should be ongoing, not just a one off activity.
- You should assess security concerns, before, during and after any activities.

### 2. OPEN DISCUSSION:

- Explain to the participants that now they will talk about predicting and identifying security threats.
- In the last lesson we focused on an interesting story from one of the participants to look at where security threats may come from. In this lesson, choose another participant story to focus on (or you may use the same story as in the previous lesson).
- Looking at that case, facilitate a discussion using these questions as a guide:
  - Can you think of ways that this kind of threat could be predicted?
  - In other situations you have been involved in, were there any indications or warning signs that there could be a security threat?
  - Which actors were involved in this case? For example, security forces, officials, a private company or other people.

### 3. EXPLAIN EXERCISE AND DIVIDE PARTICIPANTS INTO GROUPS:

- After discussing which actors were involved in this case, ask participants who else they think is often responsible for, or involved in, threats to the security of activists.

- Choose four of these actors and write each one on a different piece of flipchart paper. Stick the four papers around the room.
- Explain that in this exercise, participants will look at these four actors and try to identify how they may impact on the security of activists.
- As this lesson is about predicting or identifying threats, participants should think about common threats that they have experienced or heard about from those four actors. Tell participants to think about the different stories that they have shared during the training. For example, police may arrest someone for collecting thumbprints on a petition.
- To do this, participants will work in four groups. Each group should go to one of the flipchart papers. They will have two minutes to think of an answer and write it down or draw a picture, then they must move on to another.
- Make sure that each group has at least one person who can read and write well.

#### 4. GROUPS IDENTIFY SECURITY THREATS:

- Explain the rules of the exercise and ask the groups to start. After two minutes, ask all groups to move on to the next flipchart. Continue like this for 15-20 minutes.
- Each group should add their own answer, and should also look at the answers that are already there. If they agree with an answer, they should add a ✓ next to it, if they do not agree they should add a ✗ next to it. If they are not sure they can add a ?
- Move around the different groups and make sure that everyone understands the exercise.

#### 5. DEBRIEF:

- During the exercise all the participants will have been reading the different flipcharts and the answers of the other groups, so there is no need to take time to present all the answers.
- To debrief the exercise, ask for four different people to summarize the answers on the four different flipcharts.

- Finish by emphasizing to participants that the reason why we are looking at these threats is so that people are more aware of how to identify common threats. If you can predict a threat before it happens, or identify it early on, you may be able to reduce the harm.
- To finish on a positive, ask for one or two participants to share a story where they have faced a problem similar to those discussed in the lesson and managed to overcome the problem, or at least minimize its effect.

### 3. ASSESSING THE SERIOUSNESS OF A THREAT

Now we have looked at where threats may come from, and what those threats may be, next we will discuss ways to assess *how serious* a threat is.

#### 3.1. WHAT DOES THE THREAT LOOK LIKE?

If someone makes a direct threat you should think about the nature of that threat. The nature of the threat can give you information about the person or group that is responsible, and how serious the threat may be. For example, if someone makes a direct and open threat in public, they obviously do not fear that they will be punished, and they may have powerful connections. This type of threat can be very serious.

This is just an example, and all situations are different. This example is here to show you ways to think about the nature of the threat and what this could mean about how serious it is. You should also think about where the threat comes from:

- Is it a powerful person, company or institution?
- Do they have support of government or security forces?
- Have they threatened other people in the past?
- Did they carry out any of these threats?

#### 3.2. VULNERABILITIES AND STRENGTHS

It is important to look at where you are strong and where you are **vulnerable**. To be vulnerable means to be weak or exposed to danger. It is important to do this because if you receive a threat to your security or your group's security, and this threat is in an area where you are vulnerable, then the risk is high. If you receive a threat in an area where you are strong, the risk is lower.

For example, suppose an activist receives a threatening phone call that makes her fear she may be killed or physically hurt. She lives in a remote area in the countryside. The *threat* is the phone call, and the *vulnerability* is that she lives far from other people. This means that the risk may be high. If the activist lived in the city, or close to a strong support network, the risk may be lower.

In order to reduce risks to your security, you need to try to reduce your vulnerabilities, and improve your strengths. This is not always easy, and sometimes may be impossible, as a vulnerability may be out of your control. You will see in the table below some factors that you may be able to influence and some that you cannot.

Risks, vulnerabilities and strengths are always changing. For example, suppose one network has a very strong member who is responsible for lots of communication and planning within the network. If he leaves the network, the network may lose some of those skills. This may have a negative impact on the network's ability to organize efficiently, and this could become a vulnerability. Likewise, you may turn a vulnerability into a strength. Look at the table below for examples of different factors and how they can be vulnerabilities or strengths.

Factor	Vulnerability or strength?
<b>Location</b>	<ul style="list-style-type: none"> <li>• Do you or members of your group live in a remote area?</li> <li>• Do you have to travel often?</li> <li>• Do you have to travel to your place of work? For example, farmland or forests.</li> <li>• Is your housing safe and secure?</li> <li>• In an emergency situation, can you get away from your home quickly? Do you have a plan for this?</li> </ul>
<b>Contacts to networks, organizations and other support</b>	<ul style="list-style-type: none"> <li>• Do you have contacts with: <ul style="list-style-type: none"> <li>▪ Family members?</li> <li>▪ Other networks in your country?</li> <li>▪ Sympathetic people in government or other influential people?</li> <li>▪ People working for or with the company?</li> <li>▪ Local and international NGOs working in your country?</li> <li>▪ Embassies, development agencies, and other international institutions working in your country that may have influence?</li> <li>▪ Networks and organizations in other countries?</li> </ul> </li> </ul>
<b>Access to information</b>	<ul style="list-style-type: none"> <li>• Do you have access to reliable information?</li> <li>• Can you keep your private information safe?</li> <li>• Can you send and receive information securely?</li> </ul>

<p><b>Communication</b></p>	<ul style="list-style-type: none"> <li>• Do you have a communication system in place between members of your group?</li> <li>• If someone is threatened or harmed, do you have a system in place for communicating the information with members of your group?</li> <li>• If there is a security alert, can you quickly share information through your group or network, even if the members are spread around the country?</li> </ul>
<p><b>Group structure</b></p>	<ul style="list-style-type: none"> <li>• Is your group large or small?</li> <li>• Is your group well organized and coordinated?</li> <li>• Do people act on their own initiative, or are all actions coordinated?</li> <li>• Does your group have a security plan?</li> </ul>
<p><b>Political situation</b></p>	<ul style="list-style-type: none"> <li>• What is the current political situation?</li> <li>• Are the authorities currently sympathetic to your concerns, or are they angry with your activities?</li> <li>• Does your activism concern any powerful interests or powerful individuals?</li> </ul>
<p><b>Legal system</b></p>	<ul style="list-style-type: none"> <li>• Do you have access to protection from law enforcement authorities such as the police?</li> <li>• Can you get assistance from the authorities?</li> <li>• Do you have knowledge of the legal system and your rights?</li> <li>• Do you have access to the legal system?</li> <li>• Will the legal system deliver justice?</li> </ul>

<p><b>Access to media</b></p>	<ul style="list-style-type: none"> <li>• Do you have access to local media and international media?</li> <li>• Do you know how to talk with the media?</li> <li>• In your group, is access to the media the responsibility of one person, or several?</li> </ul>
<p><b>Emotional support</b></p>	<ul style="list-style-type: none"> <li>• Do you have a support network that can provide help and emotional support to members of your group during stressful times?</li> </ul>

## LESSON 3: ASSESSING THE SERIOUSNESS OF A THREAT

**AIM:** Participants will be able to look at an actual or perceived threat and assess how serious that threat may be.



**MATERIALS:** Whiteboard/flipchart, markers, a piece of paper with "More Serious" written on it, a piece of paper with "Less Serious" written on it, copies of Handout 1.

**METHOD(S) USED:** Group discussion, brainstorming.

Procedure	Time Frame (in minutes)
1. Introduce information from Section 3.1	15
2. Group brainstorm	20
3. Introduce information from Section 3.2	15
4. Small group discussion	20
5. Group feedback	20
6. Debrief	20
<b>Total:</b>	<b>110</b>

## INSTRUCTIONS TO FACILITATOR

### 1. INTRODUCE INFORMATION FROM SECTION 3.1:

- Start the lesson by introducing the information from Section 3.1.

**Section 3.1** - It is important that participants understand:

- If someone makes a direct threat, they must consider the nature of that threat and think about how likely it is that the threat will be carried out.
- They should consider what exactly the nature of the threat is, as well as where the threat comes from.

### 2. GROUP BRAINSTORM:

- After this, explain to the group that they will be divided into groups and they will think of five security threats they think they face during the course of their work.
- Ask participants to use a real example. This may be something that they have already discussed during the lesson, or it may be something new. Make sure that participants understand that they can include positive examples, where the threat was avoided or overcome.
- When they have decided, they should write or draw this threat on a piece of paper.
- Each group has only five minutes to do this. After five minutes is over, ask the groups to think about how serious the threat is.
- Ask the participants to stand in the centre of the room and look at one of the walls.
- Take a piece of paper with "More Serious" written on it, and stick it on the left side of the wall. Take a piece of paper with "Less Serious" written on it, and stick it on the right side of the wall.
- The groups should now stick their different answers on the wall, according to how serious they think those threats are. More serious threats should be closer to the left, and less serious threats closer to the right.

- Let participants look at the answers for a few minutes, then ask everyone to sit down again.

### 3. INTRODUCE INFORMATION FROM SECTION 3.2:

- Introduce the information from Section 3.2, but *do not* go through the table.

**Section 3.2** - It is important that participants understand:

- As well as considering the nature of any threats to their security, it is important to consider their strengths and vulnerabilities.
- Their strengths and vulnerabilities can affect how serious a risk may be.
- If there is a threat to their security and this is in an area where they are vulnerable, the risk is higher.
- Threats, strengths, vulnerabilities and risks are always changing so it is important to keep re-assessing the situation.

### 4. SMALL GROUP DISCUSSION:

- Explain that the participants will now work in five small groups and look at some areas where they may be strong or more vulnerable, and what effect this may have on their security situation.
- If participants come from different provinces, try to make sure that the groups are made up of people from the same general area. If everyone is from the same community, you do not need to worry about this.
- Each group will look at a specific area of strengths and vulnerabilities, and will be given some questions to consider. Make sure each group has a copy of the appropriate handout.
- Tell the groups to think about the handout that they have been given, and consider what their strengths and vulnerabilities are in that area.
- If a group identifies a vulnerability, they should also think about how they can try to reduce that vulnerability.
- Group 1 will look at:
  - Location
  - Access to networks, organizations and other support

- Group 2 will look at:
  - Access to information
  - Communication
  
- Group 3 will look at:
  - Group structure
  
- Group 4 will look at:
  - Political situation
  - Legal system
  
- Group 5 will look at:
  - Access to media
  - Emotional support

### Suggested answers

- All the groups' answers will be different, but below are some examples of different strengths and vulnerabilities.

Factor	Possible vulnerability	Possible strength
<b>Location</b>	<ul style="list-style-type: none"> <li>• You live in a remote area.</li> <li>• You have to travel often, sometimes at night time.</li> <li>• Your house is not safe or secure.</li> </ul>	<ul style="list-style-type: none"> <li>• You keep your house securely locked.</li> <li>• Your neighbors also watch your property for you.</li> </ul>
<b>Contacts to networks, organizations and other support</b>	<ul style="list-style-type: none"> <li>• You are not well connected with other communities or community networks.</li> </ul>	<ul style="list-style-type: none"> <li>• You keep in communication with family and friends, and keep them informed about where you are and when you will return.</li> <li>• You have some contacts with local officials.</li> </ul>

<b>Access to information</b>	<ul style="list-style-type: none"> <li>You do not always have access to reliable information.</li> <li>You do not have anywhere to keep your private information.</li> </ul>	<ul style="list-style-type: none"> <li>You have good contacts and they keep you up to date with reliable information.</li> <li>You are careful about sharing information, and only share sensitive information with people you totally trust.</li> </ul>
<b>Communication</b>	<ul style="list-style-type: none"> <li>You have no system or plan in place for communicating with other community members, partners or networks.</li> </ul>	<ul style="list-style-type: none"> <li>If a threat is made, you have a plan in place to share information with friends, partners and network members.</li> </ul>
<b>Group structure</b>	<ul style="list-style-type: none"> <li>Your group is very small and isolated.</li> <li>Members of your group often act independently without consulting with other members.</li> </ul>	<ul style="list-style-type: none"> <li>Your group has many members and you are well organized.</li> <li>Your group has a security plan in place.</li> </ul>
<b>Political situation</b>	<ul style="list-style-type: none"> <li>Your activism involves powerful and well connected people.</li> </ul>	<ul style="list-style-type: none"> <li>The current political situation is stable.</li> </ul>
<b>Legal system</b>	<ul style="list-style-type: none"> <li>You cannot access the courts or legal services.</li> <li>The legal system will not deliver justice in your case.</li> </ul>	<ul style="list-style-type: none"> <li>You have some knowledge of the law and legal systems, and know how to find a lawyer if you need one.</li> </ul>

<b>Access to media</b>	<ul style="list-style-type: none"> <li>You do not know how to talk with the media.</li> </ul>	<ul style="list-style-type: none"> <li>You have good contacts with media.</li> </ul>
<b>Emotional support</b>	<ul style="list-style-type: none"> <li>You <b>do not</b> have a support network that can provide help and emotional support during stressful times.</li> </ul>	<ul style="list-style-type: none"> <li>You <b>do</b> have a support network that can provide help and emotional support during stressful times.</li> </ul>

## 5. GROUP FEEDBACK:

- Ask each group, one by one, to summarize their discussion to the rest of the class. Ask them if they identified any key vulnerabilities or strengths – and how they think the vulnerabilities can be reduced.
- Make sure to explain that this is a short exercise to get people thinking about how they can do a full assessment of their security risks. This kind of exercise should be done in much more detail and over a longer period of time.

## 6. DEBRIEF:

- To debrief the exercise, take one key vulnerability from each of the five groups and ask the participants:
  - Does this vulnerability overlap with any of the security threats that we discussed in the exercise earlier?
  - What impact does this have on the level of risk of that security threat?
  - Is there anything that you could do to try and reduce this vulnerability and therefore reduce the risk?
- Close the lesson by explaining that the following module will look in more detail at practical ways that some security risks can be minimized.

**DIFFICULT TERMS:**

1. **Pro-active:** Being pro-active means that you act *before* something happens.
2. **Re-active:** Being re-active means that you act *after* something has already happened.
3. **Risk:** There are many definitions of what a risk is, but one basic definition is: something that might happen in the future which could cause harm.
4. **Vulnerable:** To be weak or exposed to danger.

## HANDOUT 1 – LESSON 3

### Group 1

Look at the two areas below, and think about the type of work and activities that you and your community, group, or network is doing. Think about what your vulnerabilities and strengths are.

Factor	Vulnerability or strength?
<b>Location</b>	<ul style="list-style-type: none"> <li>• Do you or members of your group live in a remote area?</li> <li>• Do you have to travel often?</li> <li>• Do you have to travel to your place of work? For example, farmland or forests.</li> <li>• Is your housing safe and secure?</li> <li>• In an emergency situation, can you get away from your home quickly? Do you have a plan for this?</li> </ul>
<b>Access to networks, organizations and other support</b>	<ul style="list-style-type: none"> <li>• Do you have contacts with:               <ul style="list-style-type: none"> <li>▪ Family members?</li> <li>▪ Other networks in your country?</li> <li>▪ Sympathetic people in government or other positions of power?</li> <li>▪ People working for or with the company?</li> <li>▪ Local and international NGOs working in your country?</li> <li>▪ Embassies, development agencies, and other international institutions working in your country that may have influence?</li> <li>▪ Networks and organizations in other countries?</li> </ul> </li> </ul>

## HANDOUT 1 – LESSON 3

### Group 2

Look at the two areas below, and think about the type of work and activities that you and your community, group, or network are doing. Think about what your vulnerabilities and strengths are.

Factor	Vulnerability or strength?
<b>Access to information</b>	<ul style="list-style-type: none"> <li>• Do you have access to reliable information?</li> <li>• Can you keep your private information safe?</li> <li>• Can you send and receive information securely?</li> </ul>
<b>Communication</b>	<ul style="list-style-type: none"> <li>• Do you have a communication system in place between members of your group?</li> <li>• If someone is threatened or harmed, do you have a system in place for communicating the information with members of your group?</li> <li>• If there is a security alert, can you quickly share information through your group or network, even if the members are spread around the country?</li> </ul>

## HANDOUT 1 – LESSON 3

### *Group 3*

Look at the area below, and think about the type of work and activities that you and your community, group, or network are doing. Think about what your vulnerabilities and strengths are.

Factor	Vulnerability or strength?
<b>Group structure</b>	<ul style="list-style-type: none"><li>• Are you a member of a group, or an individual?</li><li>• Is your group large or small?</li><li>• Is your group well organized and coordinated?</li><li>• Do people act on their own initiative, or are all actions coordinated by the group?</li><li>• Does your group have a security plan?</li></ul>

## HANDOUT 1 – LESSON 3

### Group 4

Look at the two areas below, and think about the type of work and activities that you and your community, group, or network are doing. Think about what your vulnerabilities and strengths are.

Factor	Vulnerability or strength?
<b>Political situation</b>	<ul style="list-style-type: none"> <li>• What is the current political situation?</li> <li>• Are the authorities currently sympathetic to your concerns, or are they angry with your activities?</li> <li>• Does your activism concern any powerful interests or powerful individuals?</li> </ul>
<b>Legal system</b>	<ul style="list-style-type: none"> <li>• Do you have access to the protection from law enforcement authorities such as the police?</li> <li>• Can you get assistance from authorities?</li> <li>• Do you have knowledge of the legal system and your rights under it?</li> <li>• Do you have access to the legal system?</li> <li>• Will the legal system deliver justice?</li> </ul>

## HANDOUT 1 – LESSON 3

### Group 5

Look at the two areas below, and think about the type of work and activities that you and your community, group, or network are doing. Think about what your vulnerabilities and strengths are.

Factor	Vulnerability or strength?
<b>Access to media</b>	<ul style="list-style-type: none"><li>• Do you have access to media local and international media?</li><li>• Do you know how to talk with and manage the media?</li><li>• In your group, is access to the media controlled by one person, or several?</li></ul>
<b>Emotional support</b>	<ul style="list-style-type: none"><li>• Do you have a support network that can provide help and emotional support to members of your group during stressful times?</li></ul>

# PRACTICAL SECURITY: MINIMIZING RISKS

## OUTCOMES

After completion of this module, participants will:

1. Understand that taking pro-active steps to minimize risks is the best way to protect your own security.
2. Be aware of a number of basic measures they can take to reduce security risks for themselves and their group.

## 1. MINIMIZING RISKS

We have already discussed the idea of security, and ways that you can identify different security threats. In this section we will discuss some general techniques that can be used to minimize security threats. Some techniques can be used in situations where there is an actual threat, or when you predict a possible threat in the future. Some of the methods below can be used at any time and may help to prevent or at least minimize the risk of a security threat arising in the future. All of the measures below are intended to be practical and straightforward. You may not have thought of some of them before, and you may also have some other ideas which are not listed here.

The reason why we discuss these practical steps is to show how everyone can play a part in security planning and precautions. As already mentioned, it is always more effective to be *pro-active* rather than *re-active*. By taking some of these steps and acting *before* a threat becomes real, you may be able to avoid or reduce the risk.

## 2. PRACTICAL STEPS

### 2.1. SECURITY AWARENESS

It is important that activists have at least a basic knowledge about security risks and precautions. Anyone that is involved in advocacy should know how to minimize security risks to themselves and other members of their group.

For example, if your group or network organizes some kind of event such as a workshop, campaign launch, site visit or press conference, it is possible that people may be asked by authorities or security forces what they are doing. They may ask: "Why are you going to Phnom Penh? What is the purpose of your meeting?" In case this happens, it is a good idea to think about what the best response to these kinds of questions might be.

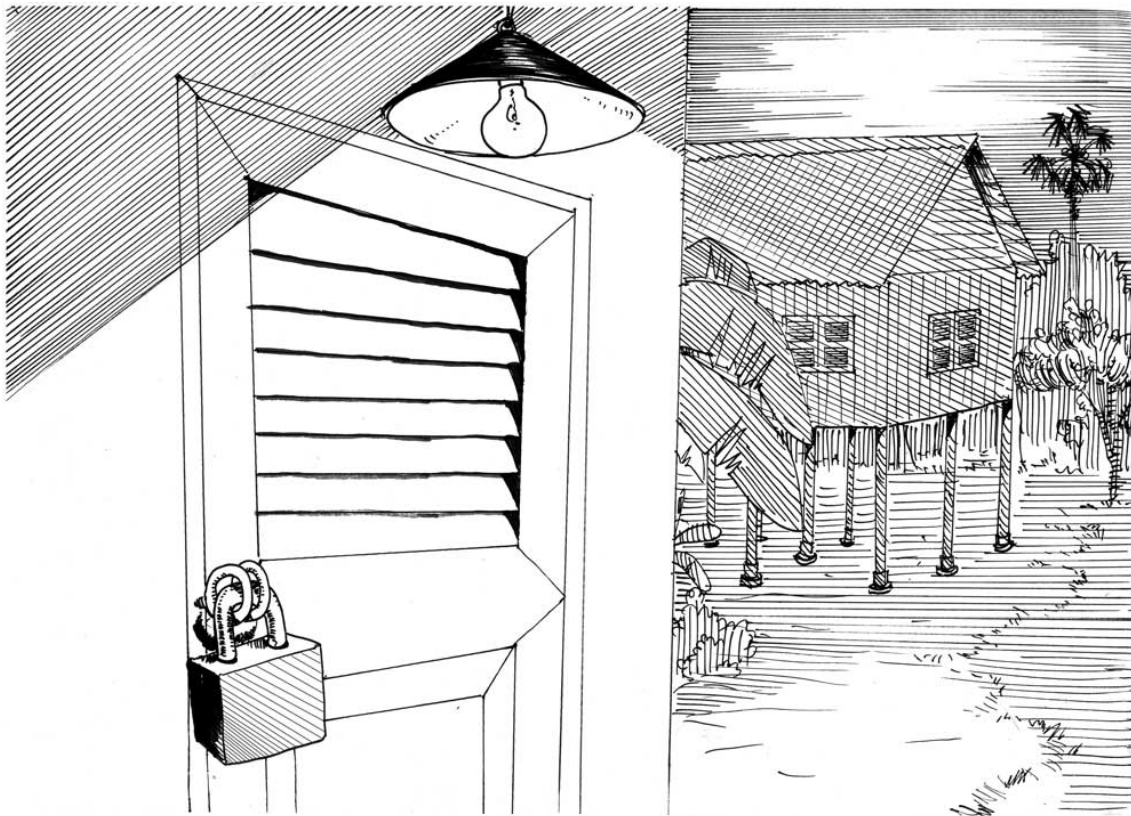
Before any event or activity you should brainstorm and discuss any possible security problems that may come up, and have a plan for how you will deal with them.

## 2.2. FAMILY AND FRIENDS

You may want to take the time to explain to your family and very close friends what exactly your work involves, especially if you think that your security is at risk. Your family may be the first people to notice if something happens to you, especially if you keep them informed of where you are going and what time you expect to return home. You may want to explain to them what they should do if, for example, you do not return home on time or if you are arrested.

## 2.3. SAFETY AT HOME

There are some simple things that you can do to improve the security of your home. For example, you should try to make sure that there is enough lighting at night, or if you think someone may try to come on to your property during the night you may want to get a dog to sleep outside. Make sure that you lock the doors to your home if possible. If you think your house does not provide enough protection you may want to sleep at the house of a friend or family member. If you think the risk is very high, you could change the place that you sleep every night or every few nights.



## 2.4. CONTACT AND COMMUNICATION

It is important to share information within your group or network if you think that there is a possible security risk. You may also want to be in contact with other networks and groups who are working on similar issues in other areas. They may have information or experiences that could be useful to you. However, although it is important to disseminate information, and scaring people with too many warnings.

If you are working on issues that affect the interests of powerful individuals or companies, you may want to make contact with NGOs working in your area to let them know about your work and any security concerns you may have. If there is a security incident they may be able to assist you or help you make contact with other people who can help. You should not rely on NGOs to solve your problems, but they may have resources and contacts that could be useful to you and your network. NGOs may be able to communicate concerns to the authorities; this will give the authorities notice that someone is monitoring the situation.

If you want to contact high level organizations such as the United Nations you may first want to talk with local or international NGOs based in Phnom Penh.

## 2.5. TRAVEL

Travelling can sometimes be risky, especially on Cambodia's dangerous roads. If you feel that your safety is at risk, you may want to consider avoiding travel at night, and always travel in a group rather than on your own. This is because if someone wants to do you harm, they could do this and make it look like a simple traffic accident.

Another good strategy is to change your routine regularly. You could leave your house at different times each day, travel home from work at different times, and even take a different route if possible. If you have to travel long distances to your workplace, fields, forests or fishing grounds, try to avoid doing this alone.

## 2.6. BE AWARE

It is important to always be aware of what is going on around you. Be aware of who might be watching you and listening to what you are saying. If something makes you uncomfortable or suspicious, you may want to discuss it with other members of your group.

Be careful about passing on sensitive information to people that you do not know well or that you do not trust. Earlier we discussed how people may use tricks to try to get sensitive information out of you, sometimes without you even realizing. Be aware that people may try to do this.

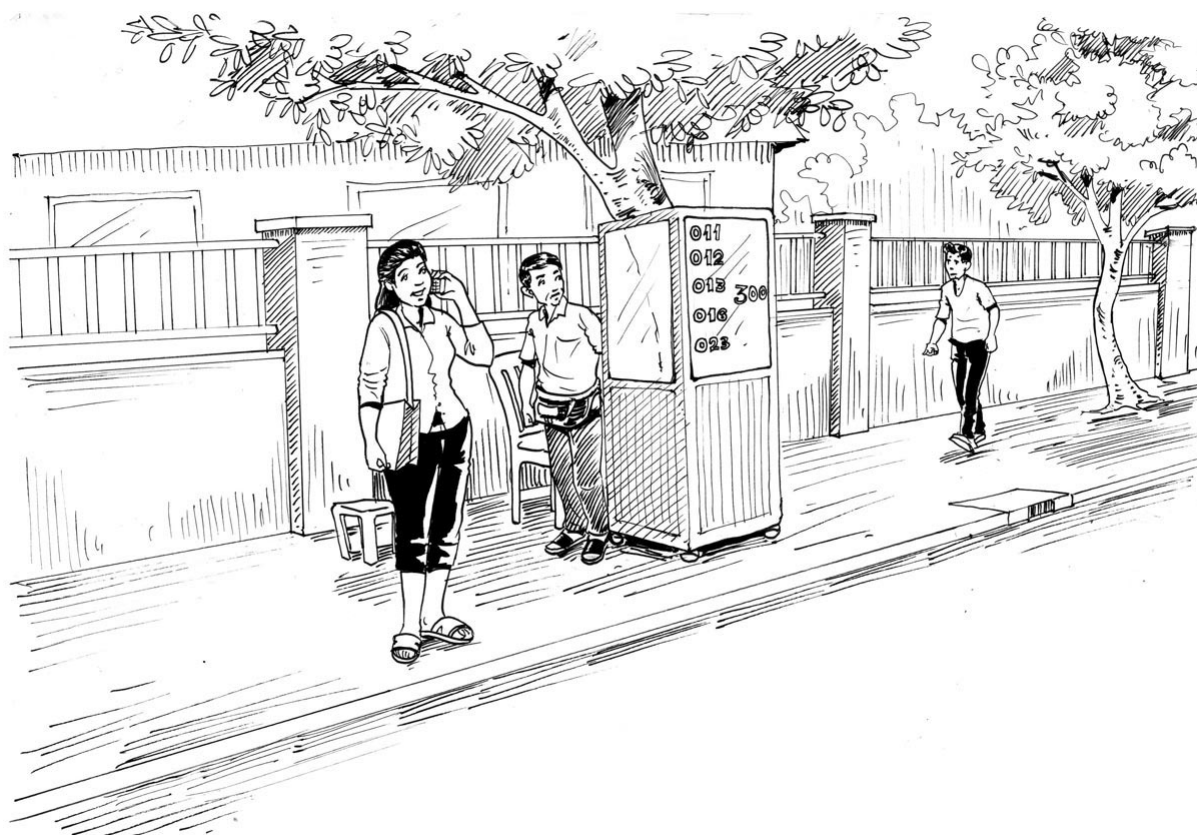
## 2.7. SAFER USE OF TELEPHONE AND EMAIL

When talking on the telephone you should always be careful about what you say. It is very easy for people to listen to your telephone calls. They may do this by just standing close to you, but there is also technology that allows people to listen in to the conversations people have on their phone – even if the conversation is far away.

If you are talking about something that you do not want other people to hear, the safest thing to do is have this discussion face to face and in a place where people cannot overhear you. If you have no choice but to talk on the phone, it is more secure to have a special number (a different phone and/or SIM card) that only a few highly trusted people know. The more people who know your number, the more likely it is that others will be able to listen in to your calls.

For the same reasons you should be careful about what you write in emails. There is technology people can use to read your emails, even though you have a password for your account. Also, it is very easy for people to print or forward your email to others, and this way any private information can become public very quickly.

In the annex of this manual is a fact sheet on information security. This contains more details about using the telephone and internet more safely, and on safer storage of documents.



## 2.8. KEEP INFORMATION SAFE

Make sure you keep all sensitive information in the safest place possible, and keep important documents in a place where you will not lose them or get them damaged. Do not throw old documents in the trash if they contain sensitive information – you should first rip them up.

## 2.9. REACTING TO THREATS

If a threat becomes real, you will have to decide how to react. In the next module we will talk about different ways to respond to a security threat.

## LESSON 1: MINIMIZING SECURITY THREATS

**AIM:** Participants will discuss some of the measures they already take to minimize security risks and learn about others that they may not yet be aware of. They will think of examples where they could use these measures in the future.



**MATERIALS:** Whiteboard/flipchart, markers.

**METHOD(S) USED:** Open discussion, sharing ideas, presentations (methodology to be chosen by participants).

Procedure	Time Frame (in minutes)
1. Open discussion	20
2. Divide participants into groups and explain exercise	5
3. Groups prepare presentations	15
4. Presentations	40
5. Debrief	20
<b>Total:</b>	<b>100</b>

## INSTRUCTIONS TO FACILITATOR

### 1. OPEN DISCUSSION:

- Open the lesson by explaining that at this point we will not discuss how to deal with specific threats, but we will look at measures that can be taken to reduce security risks in general. You can use Section 1 to help you explain this.
- Instead of telling the participants what they can do, a better way to start is to ask participants to tell each other about different measures they already take to stay safe.
- Ask participants to raise their hand if they want to add something, and encourage other participants to ask follow up questions if they like.
- Write down some good examples on the flipchart or whiteboard.
- Give participants a chance to brainstorm their ideas, and then you can add any points they may have missed from Section 2.
- In the next exercise participants will create their own presentations on how they would minimize security risks in a specific situation.

### 2. DIVIDE PARTICIPANTS INTO GROUPS AND EXPLAIN EXERCISE:

- Explain that in the following exercise, participants are going to create a presentation. The presentation should show at least three different ways that the people involved in this case could act in order to minimize any possible security risks they may face.
- Divide participants into 4 groups and give each group one of the cases listed below and in Handout 1.
- Explain that participants can use any method that they want to present their answers, but they should try to be as creative as possible. They can do something artistic, or make a role-play, write a song or create a game for everyone to join.
- Make sure that participants understand that in all the cases, no threat has yet been made. They should be thinking about ways to try and reduce the chance that a threat will arise.
- Each group will have 10 minutes to present their presentation.
- Give one of the following cases to each group:

- Group 1: A community network plans to organize a petition against economic land concessions affecting forest communities. They are worried that their action will put them at risk.
- Group 2: The residents of one village plan to demonstrate outside the offices of the provincial governor because a powerful individual has taken some of their farmland. The organizers fear that their safety may be at risk.
- Group 3: Residents of two villages have come into a land conflict with a powerful individual. He is not an official, but has connections with high ranking people. The community wants to hold on to their land, but people also fear for their safety.
- Group 4: A community network has planned a workshop for members in several different provinces. The workshop will focus on sensitive issues of land and forestry, and the organizers are worried about having problems if they go ahead with the plan.

### **3. GROUPS PREPARE PRESENTATIONS:**

- Supervise the groups as they prepare their presentations. Help them to think of creative ideas that will be interesting for the other participants to watch.
- Remind them that their presentation can be no longer than 10 minutes long.

### **4. PRESENTATIONS:**

- Ask the groups to present one at a time. After each presentation, ask the observers what they think the presenters did to show possible ways to minimize security risks. Write down each answer on the flipchart or whiteboard.
- Do this with each group, and leave the answers on the flipchart or whiteboard for the debrief.

### **5. DEBRIEF:**

- To debrief the lesson, look back at the different measures that the participants came up with for minimizing security risks. Look at the text in Section 2 above, and if there are any measures that were not discussed during these presentations, or during the earlier discussion, you can talk about them now.
- If you would like to add more detail to any of the participants ideas, you may do that too. Ask if any participants have any more suggestions.

**HANDOUT 1 – LESSON 1**

Give one to each group:

Group 1: A community network plans to organize a petition against economic land concessions affecting forest communities. They are worried that their action will put them at risk.

Group 2: The residents of one village plan to demonstrate outside the offices of the provincial governor because a powerful individual has taken some of their farmland. The organizers fear that their safety may be at risk.

Group 3: Residents of two villages have come into a land conflict with a powerful individual. He is not an official, but has connections with high ranking people. The community wants to hold on to their land, but also fear for their safety.

Group 4: A community network has planned a workshop for members in several different provinces. The workshop will focus on sensitive issues of land and forestry, and the organizers are worried about having problems if they go ahead with the plan.



# RESPONDING TO SECURITY THREATS

## OUTCOMES

After completion of this module, participants will:

1. Be aware of several different strategies that can be used in responding to security threats.
2. Understand the importance of keeping adequate documentation of security threats.
3. Know how to report an incident, and who they can report to.

## 1. HOW DO YOU RESPOND TO SECURITY THREATS?

If you or your group identifies a serious security threat, it is important to respond in an appropriate way. There are many different ways to respond to a threat, and how you respond will be different depending on your situation and the type of threat.

1. *Ignore the threat:* One way to respond to a possible threat is to ignore it. But, as we already mentioned, this is not a good way to respond to threats. Although it may make you feel safer in the short term, the threat will probably not go away and may even become more serious if you do nothing about it.
2. *Confront the threat:* A better way to respond is to confront the threat. To confront a threat does not mean you have to fight or come into conflict with the person or people making the threat – it simply means that you face the threat and decide how to deal with it.
3. *Share the risk:* Part of dealing with risks may be to share them. Individuals can be exposed and vulnerable, but confronting threats as a group may provide more protection.

As always, the most effective way to confront a threat is to be pro-active. The following are some practical steps you may want to consider in case you face a security threat. They are focused on *confronting* and *sharing* risks.

### 1.1. WHEN DO YOU RESPOND TO A THREAT?

As soon as you identify a possible threat, or as soon as a threat is made, you need to decide when and how you will react. Your reaction may be:

1. *Immediate* – If there is a very serious threat of harm happening now, you should act straight away. For example, if an activist receives a death threat, they should

act immediately to get themselves to a safe place. This may have to be done without a big discussion with others because you have a serious concern that harm is about to happen.

2. *Rapid (fast)* – This is still a fast reaction, but you may have a few hours or days to discuss what to do with partners and friends. For example, if an activist hears that they may be arrested sometime next week, they should act quickly to find out more information. This could involve talking to local officials, other community members and NGOs.
3. *Monitor and follow-up* – You may not think the threat is serious yet, but you should monitor it carefully. If the threat becomes more serious, you may want to take some action. This could be a few weeks or even months later. For example, if a community hears that a company is going to come and clear their farmland sometime soon, they should try and find more information, monitor activity in the area, and notify others. If clearing starts, then they can take further action.

## LESSON 1: HOW DO YOU RESPOND TO SECURITY THREATS?

**AIM:** Participants will look at different ways that they may respond to security threats. They will be able to consider which types of response are appropriate in different cases.



**MATERIALS:** Whiteboard/flipchart, markers.

**METHOD(S) USED:** Discussion, brainstorming.

Procedure	Time Frame (in minutes)
1. Introduce information from Section 1	15
2. Whole group discussion	15
3. Whole group discuss case studies	20
4. Debrief	10
<b>Total:</b>	<b>60</b>

## INSTRUCTIONS TO FACILITATOR

### 1. INTRODUCE INFORMATION FROM SECTION 1:

- Start the lesson by introducing the information from Section 1.

**Section 1** - It is important that participants understand:

- There are many ways that you can respond to security threats.
- Ignoring a threat is not likely to make you any safer.
- Confronting the threat is the best way to deal with it.
- If people work together and share the risk then everyone can be safer.
- Some threats need immediate action; others do not need immediate action and can just be monitored. The speed of your reaction depends on how serious the threat is.

### 2. WHOLE GROUP DISCUSSION:

- Next, write the words "ignore" and "confront" on the flipchart or whiteboard. Make sure that everyone understands the two words (be sure to explain that when we say "confront" here, we are talking about dealing with the threat – not creating conflict.)
- Ask the participants if they think it is better to *ignore* or *confront* security threats. If you have time you can write some of these answers on the board or chart, or ask a participant to help you.
- After this, write "immediate", "rapid/fast", "monitor/follow-up" on the whiteboard. Make sure that everyone understands the three terms, and explain that if you are threatened, you need to decide how you will react.
- Explain that it is important to decide how quickly you will react depending on how serious a security threat may be. If the situation is very serious but you delay, something very serious could happen. If the threat is not so serious but you react too quickly, you may scare people for no good reason.

### 3. WHOLE GROUP DISCUSSION OF CASE STUDIES:

- Explain that participants will look at a short case study and think about different responses. They should think about ways to confront the problem, and also how urgent it is to respond in that situation.

- Read out the case study below and ask the participants:
  - How could the affected people in this situation confront the problem?
  - What do you think would happen if they decide to just ignore the problem?
  - How could the affected community share the risk?
  - How urgent do you think it is for the community to respond to the threat? Do they need to react immediately, or can they wait and monitor the situation?

### CASE STUDY

A community has been in conflict with a wealthy business person for over a year. The business person claims that they now own 50 hectares of land that has traditionally been used by the community.

Recently the business person sent his company staff to clear the land, but the community protested. They blocked the company from clearing the land and eventually the company staff left. The community was organized by a strong leader, and that night, some men came to his house and warned him that if he did not stop helping the community organize he would be harmed.

The following day, police came to the community leader's house and told him he was ordered to come to the police station to answer questions.

#### 4. DEBRIEF:

- To debrief the exercise, explain to the participants that in this lesson they discussed general strategies for how and when to respond to security threats. In the next lesson they will get a chance to discuss some more detailed steps that they can take if a security threat comes up.
- Take a chance here to answer any questions the group may have before moving on.

## 2. STRATEGIES FOR RESPONDING TO THREATS

### 2.1. KEEPING RECORDS

After any immediate danger has passed, one of the first things that you should do is make a record of any security threats. Doing this soon after the event means that the facts will still be fresh in your mind and you will still remember important details. Think about the following questions:

- What happened?
- Where did it happen?
- When did it happen?
- Who was involved?
- What was the threat? (This could be a verbal threat, or just a fear of harm.)
- What is the background of the case?
- Was there any injury or damage to property?
- Were there any witnesses?
- What action did the authorities take?

You should keep this information safe and use it if you decide to report the security threat to the police, courts or to organizations. Even if you decide not to formally report the incident, it is good to have things recorded. This way if something happens again in the future you can use this documentation. In the next lesson we will discuss reporting in more detail.



## 2.2. MOBILIZE SUPPORT

As mentioned above, individuals and small groups are at greater risk when there is a security threat. After a threat you should **mobilize** support. This means making contact with those who work with or support you, explaining your situation and asking them to provide additional support to deal with the security situation. To do this you may want to contact:

- Other members of your network or group;
- Other communities who have had similar problems;
- Partner networks;
- Local organizations;
- International organizations;
- United Nations Office of the High Commissioner for Human Rights; and
- Officials and contacts in government who may be sympathetic to your problems

You may also want to talk with any contacts you have in the media, but this must be done very carefully. This is discussed more below.

The different groups listed above may be able to help you in different ways. For example, any contacts you have in government may be able to raise your concerns to higher level officials. NGOs may be able to provide you with legal advice or they may be able to keep important documents in a secure place. Other networks may be able to travel to your area and stand with you in solidarity.

Remember though, it is still not a good idea to rely only on the groups listed above. You need to continue to be active in protecting your own security.

## 2.3. MONITORING

After a threat is identified, you should **monitor** that threat. This could just mean that you meet amongst your partners regularly to discuss any developments in the situation, or it could be requesting direct monitoring from an NGO. In some cases, you may want to contact an organization to visit you or observe the situation.



*Community member and NGO workers monitor land conflict*

If you decide to do your own monitoring, you should decide who is responsible for what, and you should have in place a plan for what people should do if the situation gets worse or if there are further problems. Monitors should know who to contact and how to respond if something happens. It is useful for monitors to have cameras, but these should be used discreetly.

## **2.4. EXTRA VIGILANCE**

If there is a serious security threat, as well as monitoring the situation, you need to be more **vigilant** in general. This means that you should take precautions like those discussed earlier in the module on *Minimizing Risks*. For example, you could change your routine, travel different routes and at different times, meet at different places, and so on.

You should be extra careful not to talk about sensitive issues on the phone or by email. Anyone who feels threatened should not travel alone or at night, unless this cannot be avoided. You can also make sure that you change your routine each day so that it is harder for people to follow you and find you.

## **2.5. SAFE HOUSES AND HIDING**

Sometimes the safest thing to do is to stop whatever it is that you are doing. If you fear for your safety or for the safety of those around you, you may want to be "quiet" for a while. This could mean closing an office or cancelling an event until the situation is better.

In very serious situations people may have to go into hiding. This can mean moving to a different part of the country and staying in a **safe house**. A safe house is a place you can go to if you fear that you may be harmed or arrested. This place should be secure and only very few people should know where it is and who is staying there. If you think

you may need to use this safe house, you should try to have a plan in place for how you will get there in an emergency.

## 2.6. LEGAL ADVICE

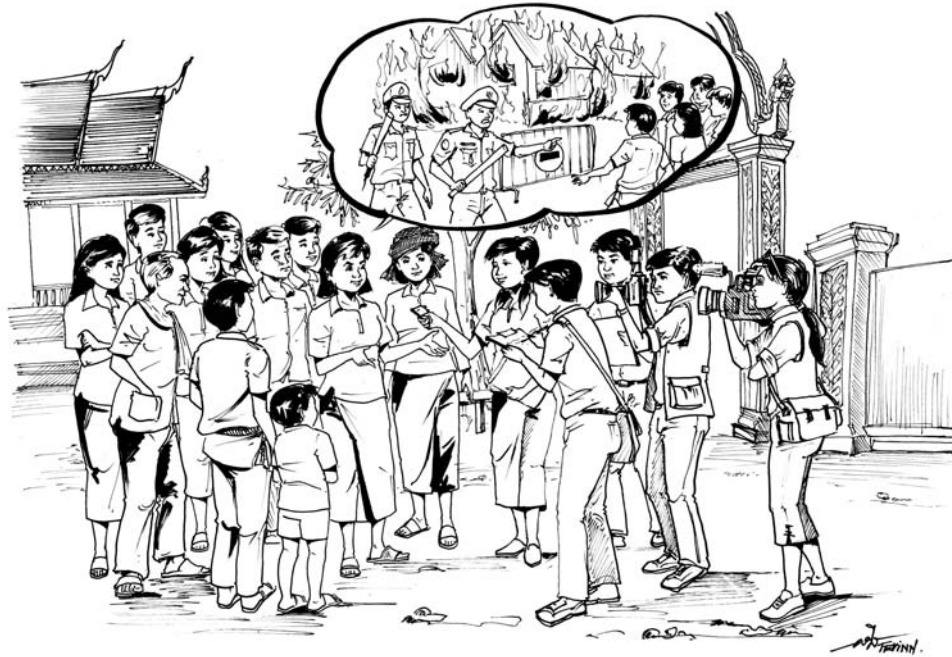
If there is the threat of legal action against you or a member of your group you may want to talk with an NGO about how to find legal advice. Some NGOs work directly on legal and human rights issues and may be able to give you some advice, others may be able to refer you on to another organization. Many activists have signed forms with NGOs that request the NGO find a lawyer to represent them in case they are arrested.



There is a factsheet included in the annex of this manual with tips on finding and working with a lawyer.

## 2.7. MEDIA

In some cases you may think that the best thing to do is reduce the threat by keeping quiet, or even stopping your activism until the situation "cools down". However, in other cases it may be better to raise the profile of the case. For example, if a member of your group has been arrested, it may help to get people's attention. One way you can do this is through the media (radio, newspapers or television), but you must be very careful about making this decision.



Sometimes the media can misrepresent your story (on purpose or accidentally) and this could be harmful to your situation. If you speak with the media you must be sure that you have a clear idea of what your aim is, and what facts you will tell them. Be sure to send the message that you are looking for a resolution to your problems, and not for conflict. If you are part of a group or network, as with any major strategy, any decision to speak with the media should be made according to your group's decision making processes, not according to an individual.

Sometimes it may be safer to ask an NGO to make a statement in the media regarding your case. Again you should be careful and make sure that the NGO represents the case the way that you want them to.

## 2.7. SOLIDARITY

As we already discussed, it is generally true that individuals and small groups of people are more vulnerable. Because of this, it is important to support your partners and network members if they face security threats. There are many ways that you can provide support. Some can be as simple as providing emotional support, such as calling them and checking how they are, and giving them someone to talk to about their concerns. You may also be able to help with monitoring on a specific case.

Your community, group or network can respond to threats with a collective statement or a collective response. In 2009, one community activist was called for questioning by a local official. In response, his whole community went with him to show support. This type of action can help improve the security situation of individuals who are targeted.

**ALWAYS CONSIDER THE FACTS OF YOUR OWN SITUATION**

All of the techniques above are just examples of action you can take in response to a security threat. There is not a single plan on how best to respond, you should always consider the facts of your own case very closely.

The strategies listed here are not the only options, and although they may help, they will not *guarantee* your safety. Some of them will not be appropriate to your situation, and some may need to be adapted to be suitable. But remember, although it may be frightening to think about some of these ideas, just thinking about them and being more prepared is a step towards making you and your group more secure.

## LESSON 2: HOW DO YOU RESPOND TO SECURITY THREATS?

**AIM:** Participants will look at different ways that they may respond to security threats. They will be able to apply these strategies to their own situation and consider which are appropriate to different cases.



**MATERIALS:** Whiteboard/flipchart, markers.

**METHOD(S) USED:** Discussion, brainstorming, drawing, presentations.

Procedure	Time Frame (in minutes)
1. Introduce information from Section 2	30
2. Small group discussion and drawing exercise	20
3. Group feedback	20
4. Debrief	10
<b>Total:</b>	<b>80</b>

## INSTRUCTIONS TO FACILITATOR

### 1. INTRODUCE INFORMATION FROM SECTION 2:

- Next, introduce the information from Section 2.

**Section 2** - It is important that participants understand:

- Different strategies that may be used in response to security threats.
- All cases are different, and the strategies that you decide to use should always be based on the situation and facts in your case.

### 2. SMALL GROUP DISCUSSION AND DRAWING EXERCISE:

- Next, divide the participants into four groups. Explain that they should each take some flipchart paper and go to a different part of the room.
- They should think about the different strategies that were just discussed for responding to threats. With this in mind they should draw a picture of an experience that they have had, or one that they have heard of, where a person or group was faced with a security threat.
- This experience can be something that affected the whole group, or if they are from different areas, it could be the experience of one member of the group. The important thing is that participants are thinking about threats, and ways that they can react to them.
- They should draw a picture of the threat, and then on a second piece of paper they should draw how the individual or group responded to the threat.
- While they are drawing the second picture, the groups should think carefully about how they responded. Tell them to think about these questions:
  - What did the people in the picture do to respond to the threat?
  - Was it effective?
  - What could they have done better or differently?

### 3. GROUP FEEDBACK:

- Each group has five minutes to present their picture to the rest of the group. First they should hold up the picture that shows the problem, and explain what happened.

- Give the other members of the group a chance to say what possible responses the people in the picture could have taken. Then let the group present their second picture.
- Ask what the outcome of the situation was. Were the responses enough to resolve the problem? What could they have done differently or better?
- These pictures will be used in the next lesson also, so ask participants to keep them safe.

#### 4. DEBRIEF:

- To debrief the exercise, quickly ask participants to summarize to you the different responses that have been discussed in this lesson. Ask them to add more if they think of any.
- Take this opportunity to remind participants about the different stages of security planning:
  - Earlier in the training we looked at the very basics of what security is, common threats that activists face, and where these threats may come from.
  - After this we considered some pro-active steps that activists can take to reduce the chance that security threats will happen.
  - In the last two lessons we talked about what to do and how to react if an actual threat is made.
- The message we have tried to get across in these lessons is of being *pro-active* at every step – from general security awareness, to identifying threats, minimizing threats and reacting to threats. It is important to be proactive before, during and after any situation where there may be a threat to your security or the security of your group.
- Next we will talk about how to report on security threats.

### 3. REPORTING INCIDENTS

As mentioned above, one of the first things you should do if you experience a threat to your security is record what happened. This information should then be used if you decide to report the incident. You may report the incident to the authorities, police, courts, your partners, NGOs, UN agencies and embassies or development agencies.

Remember to keep a record of what happened, where and when it took place, who was involved and if there was any harm to individuals or damage to property. It is up to you and your group whether or not to report an incident, and if so, who you report it to. If you do make a report, make sure to keep a copy of the report and try and get a receipt from whoever you give that report to. Remember that if you make any accusation that someone has broken the law, you must be careful. If you make a public statement about someone (in writing or spoken) and the information is untrue there is a risk that you may break the law (see module on *Legal Threats*). In some cases people are wrongly charged with this crime, so you must also consider this.

There is an example reporting form at the end of this section.

Below are some of the people that you may choose to report to:

#### 3.1. THE POLICE AND COURTS

You may decide to formally report the case to the village or commune leaders, police and the courts.

Even if you do not have much faith that your case will be heard, this may have the effect of putting the case on the official record, which is sometimes useful. If local level authorities will not accept your report, you could take it to the next level.

#### 3.2. NETWORKS AND PARTNERS

You may want to report the case to your partners or other networks. This is a more informal way of reporting security threats, but it is useful to share information between groups who may face similar threats, or may have experience in dealing with them.

As many threats go unreported, it may be a good idea to regularly share reports with other members of your group and with you partners.

#### 3.3. LOCAL AND INTERNATIONAL NGOS

You can report to NGOs formally or informally. If you just want to inform them about your situation, but do not want them to take any action, you can give them a report and ask them to keep it confidential. You can also report formally and ask for some kind of

support or intervention. NGOs may be able to help you find legal help, provide monitoring, issue statements, help you contact the media, or help to set up meetings between the parties or mediate in a dispute.

Some NGOs specialize in providing legal help, and you can see a list of these groups and how to contact them in the appendix of this manual.

### **3.4. UN AGENCIES**

You may also decide to report a case to a United Nations agency. In case of a security threat the appropriate agency to report to is the Office of the High Commissioner for Human Rights (OHCHR). The form used in this lesson, is based on an OHCHR form.

### **3.5. EMBASSIES**

You may also decide to report to the embassies of other countries that are based in Phnom Penh. You may do this to ask that the embassy discuss the case with government officials, or it may be the case that the country in question has some kind of interest in the case. For example, a company from country X could be in a joint development project with a Cambodian company. If a dispute arises and leads to threats to your security, you may want to send a report to the embassy of country X. You may want to talk with an NGO for help in contacting an embassy.

## Report Form

1. **Date of Event:** .....

2. **Place of Event:**.....village, ..... commune  
 .....district, ..... province

**3. Name(s) of person threatened:**

1....., sex: ..... , age:....., occupation:.....  
 Address:.....

2....., sex: ..... , age:....., occupation:.....  
 Address:.....

3....., sex: ..... , age:....., occupation:.....  
 Address:.....

4....., sex: ..... , age:....., occupation:.....  
 Address:.....

**4. Name(s) of person who made the threat**

1....., sex: ..... , age:....., occupation:.....  
 Address:.....

2....., sex: ..... , age:....., occupation:.....  
 Address:.....

3....., sex: ..... , age:....., occupation:.....  
 Address:.....

4....., sex: ..... , age:....., occupation:.....  
 Address:.....

**5. Name(s) of eyewitnesses:**

1....., sex: ..... , age:....., occupation:.....  
 Address:.....

2....., sex: ..... , age:....., occupation:.....  
 Address:.....

3....., sex: ..... , age:....., occupation:.....  
 Address:.....

**6. Summary of the facts:**

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

**7. Background of case**

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

**8. Summary of communications with authorities**

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

**9. Action taken by authorities**

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

Name of Reporter:

.....

Thumbprint

Date: .....

## LESSON 3: REPORTING INCIDENTS

**AIM:** Participants will know who they should report to, and what information they should include in a report. They will practice making a report.



**MATERIALS:** Whiteboard/flipchart, markers, copies of Handout 1.

**METHOD(S) USED:** Groups practice filling out report form.

Procedure	Time Frame (in minutes)
1. Introduce information from Section 3	20
2. Groups write report	20
3. Debrief	20
<b>Total:</b>	<b>60</b>

## INSTRUCTIONS TO FACILITATOR

### 1. INTRODUCE INFORMATION FROM SECTION 3:

- Start the lesson by introducing the information from Section 3.

**Section 3** - It is important that participants understand:

- The first thing you should do after danger has passed is to write down what happened. If this is difficult for, you should find a trusted person to help you write it down.
- This record should be kept safe in case you decide to report the incident.
- Security threats can be reported to various different people, groups or institutions.

### 2. GROUPS WRITE REPORT:

- Divide the class back into the same groups as in the previous lesson and give each group a sample report form (Handout 1).
- Explain to the participants that they should think about the security problem that they discussed in the last lesson and right it up in a report form. If they do not have enough detail about their own case they can use the example case below.
- The aim of the exercise is to give participants practice looking at a case and putting the facts into a report. Explain that the report they do in this lesson does not have to be perfect, and participants do not need to worry too much about the language and neatness. This is just an opportunity for participants to practice identifying the most important information to put into a report.
- If the participants would rather report on a fictional case they can use the case below:

#### FICTIONAL CASE

On 5 May 2010, three community activists living in village A, commune B, located in Kratie Province, received serious threats to their physical safety. Mr. Sek Theara (age 42), Mr. Kham Sophat (34) and Ms. Sao Neary (36) were returning from their fields one day when they were stopped by a group of men. The men warned them that if they did not stop their activism, they would be hurt. The men were armed, but wore no uniforms and did not identify themselves.

Two farmers working nearby saw the incident, their names were Mr. Kong Neth (27) and Ms. Ny Sothida (31).

The community has been involved in a land dispute with a powerful businessman for over 2 years. The businessman says that he bought 100 hectares of land and plans to grow rubber trees there. However, the people have farmed that land for over 15 years, and depend on that land to feed themselves and their families.

They have complained to the Cadastral Commission and provincial court and appealed to the Ministry of Interior, the Ministry of Agriculture, and the National Assembly in Phnom Penh, but there has been no response and no solution to their problem.

### 3. DEBRIEF:

- To debrief the lesson, ask the participants:
  - Why is it important to document any violations or security threats?
  - What is the key information that should go into a report?
  - Who can you send your report to?
- If you have time you can ask participants what they think are the positives and negatives of reporting an incident to the different groups discussed earlier.

## DIFFICULT TERMS:

1. **Mobilize:** To mobilize means to get your supporters organized and moving. If there is a security threat you may want to brief your friends and partners and ask them to be ready if the situation does not improve. They can then support you or stand with you in solidarity.
2. **Monitor:** Monitor means to watch something closely. You can monitor a security situation by being present in the area, watching what is happening, making notes and taking pictures.
3. **Safe house:** A house or place that someone can go to in an emergency situation if they fear that they may be arrested or harmed. It should be safe and secure and only a very few people should know where this place is.
4. **Vigilant:** Being vigilant means that you are alert and aware. For example, when we are talking about security, this can mean being aware of who may be watching you, following you or listening into your discussions.

**HANDOUT 1 – LESSON 1**

1. **Date of Event:** .....

2. **Place of Event:** .....village, ..... commune  
 .....district, ..... province

**3. Name(s) of person threatened:**

1....., sex: ....., age:....., occupation:.....

Address:.....

2....., sex: ....., age:....., occupation:.....

Address:.....

3....., sex: ....., age:....., occupation:.....

Address:.....

4....., sex: ....., age:....., occupation:.....

Address:.....

**4. Name(s) of person who made the threat**

1....., sex: ....., age:....., occupation:.....

Address:.....

2....., sex: ....., age:....., occupation:.....

Address:.....

3....., sex: ....., age:....., occupation:.....

Address:.....

4....., sex: ....., age:....., occupation:.....

Address:.....

**5. Name(s) of eyewitnesses:**

1....., sex: ....., age:....., occupation:.....

Address:.....

2....., sex: ....., age:....., occupation:.....

Address:.....

3....., sex: ....., age:....., occupation:.....

Address:.....

**6. Summary of the facts:**

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

**7. Background of case**

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

**8. Summary of communications with authorities**

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

**9. Action taken by authorities**

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

Name of Reporter:

.....

Thumbprint

Date: .....

# LEGAL THREATS: INCITEMENT, DEFAMATION & FALSIFICATION OF INFORMATION

## OUTCOMES

After completion of this module, participants will:

1. Know that human rights defenders and activists around the world often face the threat of unfounded legal charges.
2. Understand the law on incitement, defamation and falsification of information.
3. Be able to look at example cases and identify whether or not it is a case of defamation, incitement, or falsification of information.

## 1. COMMON LEGAL THREATS TO HUMAN RIGHTS DEFENDERS

Recently there has been an increase in the number of criminal charges filed against activists. These charges have included criminal damage, assault, vandalism and trespass. Often very little evidence is produced against the person who is charged. If a criminal charge is made against someone but has no basis in law or is not supported by evidence, it is sometimes called an unfounded criminal charge. In many countries human rights defenders face unfounded criminal charges.



Recently in Cambodia there has been an increase in cases of people being charged with incitement, defamation or falsification of information. The original idea behind creating these laws was to protect people's reputations and also keep order and peace. However, some people are concerned that they are now being used to silence people who speak out about human rights abuses, or who find themselves in a conflict with a powerful person.

It is useful to know exactly what the law says about these offences for two reasons:

- In your advocacy you will be able to make sure that in your words and actions you stay within the law; and
- If you are unfairly charged, you will be able to argue your case more strongly.

The following information is based on the new Criminal Code of 2010.

## 1.1. INCITEMENT TO A CRIME

**Incitement** is when somebody says, writes or broadcasts something that encourages others to commit a crime.<sup>1</sup> Incitement can be committed through verbal statements, books, films, posters and any other form of statement, as long as the statement is made in public. Incitement is a criminal offence which can be punished by a fine up to 4,000,000 riel or up to 2 years in jail.<sup>2</sup>

Some people who have spoken out in public against a powerful individual or helped others to organize about a land conflict have been improperly charged with incitement. The law says that incitement *only* happens when someone encourages another person to commit a crime.

It is not illegal to speak to people (including the media) and tell your story honestly and correctly or to encourage other people to defend their legal rights within the law. In the same way, it is *not illegal* to collect signatures or thumbprints on a petition.

---

<sup>1</sup> Cambodian Criminal Code 2009, Article 494.

<sup>2</sup> Cambodian Criminal Code 2009, Article 495.

## IS IT INCITEMENT?

The two stories below are fictional. The first is an example of incitement, the second is not.

A factory on the outskirts of Phnom Penh has run out of money and the managers have decided to close it down. The workers arrive to start work on Monday morning and find the gates locked. They are angry and worried that they have lost their jobs. Someone starts a rumor that the managers will not pay the previous month's salary. A group of angry workers start to protest and encourage the others to break down the gate and steal equipment from the factory. The workers break into the factory and together take materials and equipment.

*This is an example of a group of people encouraging (or inciting) others to commit robbery. This is incitement.*

Chenda lives in a village in northwest Cambodia. She is the lawful possessor of her land, as are most of her neighbors. Recently a company was given a big Economic Land Concession (ELC) to grow sugarcane on many thousands of hectares of land. This meant that the villagers lost a lot of their farmland. They decided to organize to try and get their land back or at least get some compensation, so they wrote letters, filed complaints and talked with media about their land dispute. Chenda was a strong leader and organized much of the advocacy.

*This is not incitement. Even though Chenda was the person who led the community, she cannot be charged with incitement as she only encouraged people to do things which were within the law, such as filing complaints.*

*It could only be incitement if she encouraged someone to do something which is illegal crime. If she encouraged people to act violently or destroy the property of the company she may have committed incitement, but encouraging someone to exercise their legal rights is not incitement.*



## 1.2. DEFAMATION

**Defamation** is when a person makes an accusation about another person or institution that harms the reputation of that person or institution. To be defamation the accusation must be made *in public* and must be made *in bad faith*.<sup>3</sup>

Defamation can be committed through verbal statements, books, films, posters and any other form of public statement. Some people who have criticized powerful individuals have been improperly charged with defamation.

In many countries that have laws on defamation, the truth is a defense. This means that even if you say something in public that harms someone's reputation, if the information is true, it cannot be defamation. For example, Vichet found out that Bora was stealing some money from his workplace. He told several people about this, and Bora complained to the police that Vichet committed defamation. In fact, the story is true. In many places this could not be defamation, because all Vichet did was speak the truth.

It is not clear in the Cambodian law if truth is a defense, which means the law could be used to restrict freedom of speech – even if the speaker is telling the truth.

Although it is not clear if the truth is a defense – you should always speak the truth in public. If you are not completely sure about the facts of a case, you should not make any accusation that could turn out to be false.

<sup>3</sup> Cambodian Criminal Code 2009, Article 305.

No one can be sent to jail for defamation but they can be punished with a fine of 100,000 to 10,000,000 riel.<sup>4</sup>

### IS IT DEFAMATION?

The two stories below are fictional. The first is an example of defamation, the second is not.

Makara is involved in a land dispute over the border of his land with a neighboring landowner. The dispute has been ongoing for some time, and Makara is getting very angry with his neighbor. Last week they argued again, and later Makara printed posters making accusations about his neighbor being a criminal and involved in corruption with local officials. These accusations were not true. Makara printed several posters and stuck them around the village.

*By printing and posting these posters Makara may have committed defamation. The statements were not true, and he did this in bad faith to harm the reputation of his neighbor.*

Sovanna has been in a land dispute with a powerful business person for several months. Last week the business person sent some men to bulldoze and clear part of Sovanna's land and put up a fence. Sovanna has documents that prove she is the lawful possessor of her land and she has pictures of the business man's employees pulling down the trees and putting up a fence. Many other people in the village also saw the company employees taking the land. Sovanna calls the local radio and explains what happened. Sovanna has tried to resolve the problem through the courts, but the court has not dealt with the dispute. She decided to speak to the media because she was desperate and wanted to protect her land. Her statement is reported in the newspaper and this makes the business man very angry. He files a complaint at court saying that Sovanna defamed him.

*In this case Sovanna has proof that what she said to the journalist was true. Although it is not clear if the truth is a defense to defamation, she had no bad faith and did not make these statements to harm the businessman's reputation. She simply wanted to protect her land.*

### 1.3. FALSIFICATION OF INFORMATION

According to the law, it can be illegal for someone to spread information that is:

- a) not true; and
- b) that makes the public believe that "destruction, deterioration, or damage to persons will occur".<sup>5</sup>

<sup>4</sup> Cambodian Criminal Code 2009, Article 305.

<sup>5</sup> Cambodian Criminal Code 2009, Article 425.

This is called **falsification of information** (under the previous Criminal Code this was called *disinformation*). This law exists to protect public order, and stop people from spreading false information that may disturb the peace. However, it is not entirely clear and some people are worried that it can be interpreted very widely.

Under the previous law on disinformation, the accused person had to have acted in a malicious way – here this is not a requirement. This means that you may be commit falsification of information without ever intending to cause harm. The previous law also required that the false information disturbed the peace (or was likely to disturb the peace). This is not a requirement in the new law.

Falsification of information can be punished with a fine of 2,000,000 to 4,000,000 riel or 1 to 2 years in prison.

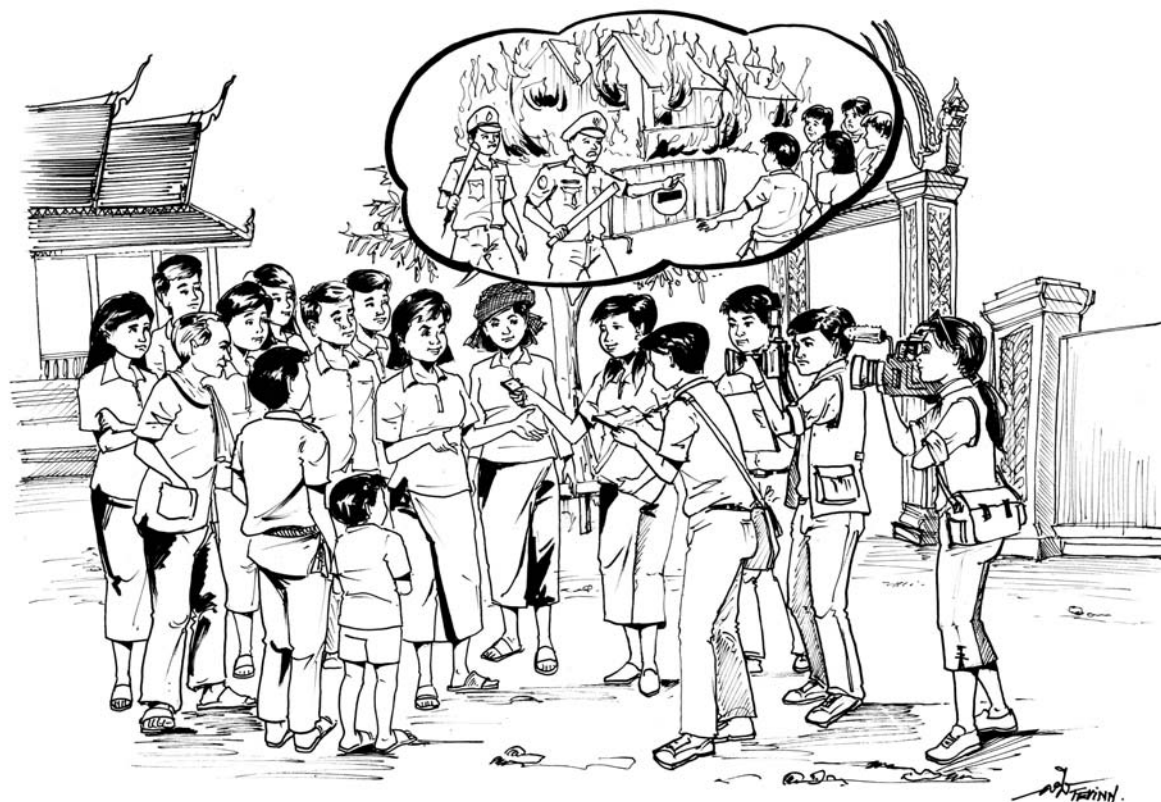
### IS IT FALSIFICATION OF INFORMATION?

The story below is fictional. It is an example of falsification of information.

Channeth lost his job working in a factory and was angry with the owner. To get revenge he made up an untrue story that the company was not going to pay employees' wages this month and was breaking other labor laws. He made leaflets with this story on and distributed them to many people in the area because he wanted to harm the reputation of the company and make the other workers angry.

*This is falsification of information because a) it was not true, and b) it may lead the public to think that harm will come to the workers.*

However, if someone makes a public statement which is true, or a statement that is not likely to make people fear that "destruction, deterioration, or damage to persons will occur", *it is not falsification of information.*



It is important to remember that the laws on incitement, defamation and falsification of information can be interpreted very broadly, and they are sometimes misused. For this reason, in order to try and minimize the risk of being charged, it is important to always be careful about the way you talk and write about sensitive subjects or events.

# LESSON 1: INCITEMENT, DEFAMATION AND FALSIFICATION OF INFORMATION

**AIM:** Participants will know that legal threats are often used to try and silence Human Rights Defenders and activists. They will understand in more detail the laws of defamation, incitement and falsification of information. They will be able to identify examples of these offences.



**MATERIALS:** Copies of Handout 1, whiteboard or flipchart, markers.

**METHOD(S) USED:** Role-play, story, large group discussion.

Procedure	Time Frame (in minutes)
1. Introduce information from Section 1	45
2. Role-play, story and discussion	30
3. Debrief	15
<b>Total:</b>	<b>90</b>

## INSTRUCTIONS TO FACILITATOR

- *Before the lesson starts* make sure that you and another facilitator are prepared to act out the short role-play below in front of the participants. If there is only one facilitator, you can ask a participant to act in the role-play with you but make sure you prepare together before this lesson.

### 1. INTRODUCE THE INFORMATION IN SECTION 1:

**Section 1** - It is important that participants understand:

- Human rights defenders and activists around the world often face the threat of legal charges because of the work that they do.
- Common charges include defamation, incitement and falsification of information.

- This may be a difficult topic for some participants to follow, especially the different elements of defamation, incitement and falsification of information. Make sure to explain the three charges clearly and slowly.
- After each offence, there is a box that gives examples. After you explain an offence and the examples, have a few minutes for question and answer, then move on to the next offence.
- For example, after Section 1.1 on incitement there is a box containing two examples. Explain these examples and then have a short question and answer session to make sure that everyone understands. Then you can move on to Section 1.2 on defamation. Do the same here before moving on to falsification of information.

### 2. ROLE-PLAY, SHORT STORY AND DISCUSSION:

- Explain to the participants that they will watch a short role-play and that they should watch and listen carefully. Explain that the role-play shows an emotional community leader talking with a journalist about a land conflict.
- You should do the roleplay with a co-facilitator, or if you are training alone you should do this with a participant. Make sure that you prepare the participant before the lesson though.
- Act out the following role-play:

## ROLE-PLAY INSTRUCTIONS

One person will act as the community leader and one person will act as a journalist. The community leader is very emotional.

### Scene 1:

The community leader calls the journalist to ask him/her to come to visit the community so he/she can explain that the community is being threatened with eviction.

### Scene 2:

The journalist comes to meet the community leader and they have a conversation. During this conversation, the journalist asks the community leader to explain the situation and who is threatening the community.

During the conversation, the community leader explains the following:

- There are two hundred families in the community, and they have lived there peacefully since the 1980s.
- Six months ago they were told to leave by local authorities because a company now owns their land.
- The company owner is Yang Leang. He is very powerful and he is trying to steal the land. He is a thief.
- Last week the company workers came to the community, beat people and destroyed property.
- The community has been told to move 25 kilometers away.
- The community will do everything to defend its land – the company does not respect the law so neither will we!
- Finally, the community leader shows the journalist a petition thumb-printed by many people. The petition says: “Stop the thief Yang Leang from stealing our land!”

- After the role-play is finished, explain that the description given by the community leader was very emotional. He made some mistakes and made some accusations about people that could get him into trouble.
- Explain that you will now read the true story of the community. You may also give out the handout to participants (Handout 1) or ask a participant to read the story.

## THE COMMUNITY'S TRUE STORY

Two hundred families in a community in Phnom Penh have lived peacefully on their land since the 1980s. Six months ago they were told by local authorities that a company now owns their land and they have to leave. The company owns land 15 kilometers away and has told the community that it should move to live on that land and that it will give each family \$500 to build a house.

Last week, company workers came onto the community's land and tried to pressure families into moving away. They told the community members that if they did not move to the land 15 kilometers away their houses would be demolished and they would get nothing.

The community does not know who owns the company but according to rumors, the owner is a powerful official called Yang Leang.

The community does not want to move away and believes they have the right to stay on their land in Phnom Penh. The community wants to avoid being evicted from their land.

- After reading the story, ask the participants the following questions:
  1. What do you think about the way the community leader communicated with the journalist?
  2. After hearing the story of the community, do you think there were any problems with the way the community leader spoke with the journalist or any problems with the information he gave?
  3. What are the possible dangers of this? Do you think he/she could be accused of incitement, defamation or falsification of information?

### **Suggested Answers:**

1. Participants might comment that the community leader was very emotional. Some may think this is a good thing, and some might think he or she spoke too strongly. Participants might comment that the community leader exaggerated or was not completely honest about the following:
  - a. He said that Yang Leang is the owner of the company but this is just a rumor. You should only make a statement like this if you are sure about the facts.

- b. He said that Yang Leang was a thief and this was also written on the petition. This could possibly be defamation.
  - c. He said that last week, company workers hit people and destroyed their property. In the story the company workers did not hit community members or destroy anything.
  - d. He said that the resettlement land is 25 kilometers away but in the story it is 15 kilometers away.
  - e. He also said that as the company does not respect the law, so neither will the community.
2. The possible dangers of this are that the community leader could be charged with a criminal offence. Calling Yang Leang a thief could lead to a charge of *defamation*. Saying that the community would do anything to defend its land and would not respect the law could lead to a charge of *incitement*. Saying that the military beat people and destroyed property could also be *falsification of information*.

### 3. DEBRIEF:

- Begin the debrief by asking participants to explain to you what the three offences of *incitement*, *defamation* and *falsification of information* are.
- Ask three different participants to give you a definition of each offence.
- If there is time, ask another three participants to give you an example of that offence being committed.
- Ask participants to think back to the role play that they looked at in this lesson. They have already discussed what the community leader did wrong. Ask them to suggest ideas of how they think he could have behaved differently in order to minimize the risks of being charged with one of the offences discussed in this lesson.
  - Explain to participants that it is very important to be honest when talking to the media.
  - If you are not absolutely sure if something is true you should not say it.
  - Instead the community leader should have told the journalist that it was very difficult to get information about the company. This way he could still tell the community's story, but hopefully avoid being charged with an offence if his information is wrong.

- If the community leader said that the people would peacefully and lawfully defend its rights to the land he could hopefully avoid being charged with incitement.
- If there is time you can ask for two volunteer participants to perform the role-play again but this time thinking carefully about how they should communicate with the media. The person acting as the community leader should perform the role-play in a way that will avoid being charged with defamation and incitement.

## DIFFICULT TERMS:

1. **Defamation:** When a person makes an accusation about another person or institution that harms the reputation of that person or institution. To be defamation the accusation must be made *in public* and must be made *in bad faith*.
2. **Falsification of information:** Spreading information that is: a) not true, and b) that makes the public believe that "destruction, deterioration, or damage to persons will occur".
3. **Incitement:** Incitement is when somebody says or writes something that encourages others to break the law.

**THE COMMUNITY'S TRUE STORY**

Two hundred families in a community in Phnom Penh have lived peacefully on their land since the 1980s. Six months ago they were told by local authorities that a company now owns their land and they have to leave. The company owns land 15 kilometers away and has told the community that it should move to live on that land and that it will give each family \$500 to build a house.

Last week, company workers came onto the community's land and tried to pressure families into moving away. They told the community members that if they did not move to the land 15 kilometers away their houses would be demolished and they would get nothing.

The community does not know who owns the company but according to rumors, the owner is a powerful official called Yang Leang.

The community does not want to move away and believes they have the right to stay on their land in Phnom Penh. The community wants to avoid being evicted from their land.



# THE LAW ON PEACEFUL DEMONSTRATION

## OUTCOMES

After completion of this module, participants will:

1. Know what a demonstration is.
2. Be aware of the key points of the laws related to peaceful demonstration.
3. Be aware of the process for notifying authorities about a planned demonstration.
4. Be aware of the responsibilities of demonstration organizers.

## 1. WHAT IS A DEMONSTRATION?

A **demonstration** is when a group of people gather in public in order to make their opinion known on a political issue or an issue that they feel very strongly about. For example, a demonstration could be held to object to a particular government policy, or the action of an official or a company. Demonstrations may also be held in support of a particular issue or policy. Some demonstrations which have happened in Cambodia over recent years include:

- Garment factory workers protesting factory closure and demanding their wages be paid;
- Trade union members and NGO staff marching in memory of the assassination of a trade union leader;
- A gathering of hundreds of people in central Phnom Penh to show support for the Preah Vihear temple being made a UNESCO site; and
- Communities threatened with eviction gathering outside the Phnom Penh City Hall to call for negotiations.

Demonstrations can take many forms, often they involve a group of people marching from one place to another. Sometimes demonstrators will make a statement or deliver a petition. Sometimes they will stand outside an office, factory or ministry.

The right to demonstrate *peacefully* is protected by law in the Cambodian Constitution. A new law called the *Law on Peaceful Demonstration* was passed in late 2009 replacing the older demonstration law from 1991.

If you are going to be involved in a demonstration, it is important that you are aware of what the law says about demonstrations. This is especially true if you are helping to organize the demonstration. An important part of minimizing security risks is understanding what the law says, and making sure that you act within the law. It is also important that you know some basic strategies for staying safe if you are involved in a demonstration.



## 2. WHAT DOES THE LAW SAY ABOUT DEMONSTRATIONS?

Cambodian law protects your right to demonstrate. The Constitution protects the right to non-violent demonstration, and states that this should be regulated by law.<sup>6</sup> This law is called the Law on Peaceful Demonstration.

### 2.1. ORGANIZING A DEMONSTRATION

The new law states that the "organizers" of a demonstration must notify the authorities that a demonstration is planned. A **notification** should be submitted in writing to the provincial/municipal authorities at least five working days (that means five days on which government offices are open) before the planned demonstration. The notification should include:

<sup>6</sup> The Constitution of the Kingdom of Cambodia, Article 37.

1. Names and addresses of at least three organizers and copies of their ID cards;
2. Explanation of the purpose of the demonstration; and
3. The date, time and length of the demonstration. This includes which streets the demonstration will pass through, and how many people and vehicles will be involved.<sup>7</sup>

The law says that the authorities should "respond positively" unless:

1. The demonstration is planned on an important national holiday or festival; or
2. The authorities have reliable information that the demonstration may cause danger or seriously harm security, safety and public order.<sup>8</sup>

The authorities have three working days to respond to the notification. If they do not respond in three working days, according to the law this means that they do not object to the demonstration and that it may proceed as set out in the notification letter.<sup>9</sup> If the authorities deny **permission**, the organizers should still have an opportunity to discuss the decision with them and try to come to an agreement on how the demonstration will be conducted. If there is still no agreement, the case should be referred to the Ministry of Interior for a final decision.<sup>10</sup>

#### NOTIFICATION OR PERMISSION?

The law says that organizers only need to give *notification* that a demonstration will happen. It does not say that they need to *ask permission*. Authorities can only prevent a demonstration if there are serious concerns about safety and public order. This is normal in most countries, and although everyone has a right to expression and to demonstrate, they cannot use this in a way that harms other people or other people's property.

The authorities should only deny a demonstration in cases when it is clear that allowing the demonstration to go ahead will cause a serious threat to security and public order.

<sup>7</sup> Law on Peaceful Demonstrations 2009, Articles 6 & 7.

<sup>8</sup> Law on Peaceful Demonstrations 2009, Article 9.

<sup>9</sup> Law on Peaceful Demonstrations 2009, Article 10.

<sup>10</sup> Law on Peaceful Demonstrations 2009, Article 11 & 12.

## **2.2. RESPONSIBILITIES OF DEMONSTRATION ORGANIZERS**

The law says that the organizers of any demonstration have a responsibility to take steps so that the demonstration takes place peacefully. The organizers must also:

1. Inform participants in the demonstration of their responsibilities to stay within the agreed area and to start and end the demonstration at the agreed time;
2. Talk and cooperate with the local officials and other authorities to make sure the demonstration remains peaceful; and
3. Keep to the agreed time and place(s) for the peaceful demonstration to take place.<sup>11</sup>

If a demonstration organizer fails to follow these steps they may be given a written warning, but the law does not set out any other penalties.

If any demonstrator commits theft, destruction of property or if anyone behaves violently, the individual and anyone who acts with them are responsible for their own actions and may be arrested and charged with a criminal offence.<sup>12</sup>

## **2.3. RESPONSIBILITIES OF THE AUTHORITIES**

The authorities also have responsibilities. As long as a demonstration is peaceful, the authorities must act to protect those people taking part. The authorities cannot interfere as long as the demonstration remains peaceful and as long as the proper notification was given by the organizers.<sup>13</sup> Authorities responsible for security must wear uniforms, with their name and identity codes displayed.<sup>14</sup>

However, if a demonstration turns violent, the authorities can immediately stop it. Also, if the organizers of a demonstration fail to give the authorities proper notice of the demonstration, it may be broken up even if it is peaceful.<sup>15</sup> This means that any spontaneous (unplanned) demonstration can legally be broken up by the authorities.

---

<sup>11</sup> Law on Peaceful Demonstrations 2009, Article 16.

<sup>12</sup> Law on Peaceful Demonstrations 2009, Articles 25 & 26.

<sup>13</sup> Law on Peaceful Demonstrations 2009, Article 17.

<sup>14</sup> Law on Peaceful Demonstrations 2009, Article 19.

<sup>15</sup> Law on Peaceful Demonstrations 2009, Article 20.

## LESSON 1: THE LAW ON PEACEFUL DEMONSTRATION

**AIM:** Participants will be aware of key points of the new Law on Peaceful Demonstration, including the procedure for notifying the authorities and the roles of the organizers and authorities.



**MATERIALS:** Whiteboard or flipchart, markers.

**METHOD(S) USED:** Open discussion and brainstorm, small group discussion.

Procedure	Time Frame (in minutes)
1. Introduce the information from Section 1	10
2. Short discussion on demonstrations	15
3. Introduce the information from Section 2	20
4. Groups review the roles and responsibilities of demonstrators and the authorities	15
5. Group feedback	30
6. Debrief	10
<b>Total:</b>	<b>100</b>

## INSTRUCTIONS TO FACILITATOR

### 1. INTRODUCE INFORMATION FROM SECTION 1:

- Start the lesson by introducing the information from Section 1.

**Section 1** - It is important that participants understand:

- What a demonstration is.
- The right to peaceful demonstration is protected by the Cambodian Constitution.

### 2. SHORT DISCUSSION ON DEMONSTRATIONS:

- Facilitate a short discussion on the participants' knowledge and experiences of demonstrations. Use the following questions to encourage the discussions:
  - Why do people organize demonstrations?
  - Do you think you have the right to demonstrate?
  - Has anyone here been involved in a demonstration before?
  - Do you think it was effective?
  - Do you think that the law protects your right to demonstrate, or limits your right to demonstrate?
- Explain that during this lesson, participants will have the chance to discuss these ideas and learn more about what the Law on Peaceful Demonstrations says.

### 3. INTRODUCE INFORMATION FROM SECTION 2:

- After the discussion introduce the information from Section 2.

**Section 2** - It is important that participants understand:

- The law that covers demonstrations is called the Law on Peaceful Demonstrations.
- There is a procedure for notifying the authorities about any planned demonstration.
- Demonstration organizers have responsibilities under the law to take steps to keep the demonstration peaceful and within the agreed route and time.
- Authorities have responsibilities under the law to protect peaceful demonstrators.

**4. GROUPS REVIEW THE ROLES AND RESPONSIBILITIES OF DEMONSTRATORS AND AUTHORITIES:**

- Next, explain that groups will look at different groups involved in a peaceful demonstration and think about what roles and responsibilities they may have.
- Divide the Participants into four groups, and ask each group to consider the rights, roles and responsibilities of *one* of the following:
  - The demonstrators
  - The organizers of the demonstration
  - The provincial/municipal authorities
  - The police and security forces
- Tell them to think about what they just learnt in the lesson, and also to think about their own ideas and experiences.
- Give each group a flipchart paper and ask them to draw pictures that show their answers. For example, the group focusing on demonstrators could draw a picture that shows that all Cambodians have the right to demonstrate. They should draw a different picture for each right or responsibility.
- Move around the groups and make sure that everyone understands the task. If any groups are finding the task difficult you may help them and suggest ideas from the Suggested Answers below.

**Suggested answers:**

*1. The demonstrators*

Everyone has the right to demonstrate non-violently and this is protected by the Constitution and the Law on Peaceful Demonstration.

This right must be used in a peaceful way, and people cannot demonstrate violently, cause damage to property or harm to people, and cannot cause a serious danger to security.

## *2. The organizers of the demonstration*

The organizers have the same rights and responsibilities as other demonstrators, but they also have the responsibility to give notification to the authorities about any planned demonstration.

Organizers must provide their name, address and copies of ID cards to the authorities, as well as a description of the planned demonstration and an explanation of its purpose.

Organizers also have the responsibility to inform demonstrators to keep within the agreed time and place for the demonstration to take place, and they also have a responsibility to cooperate with the authorities to help make sure the demonstration remains peaceful.

## *3. The provincial/ municipal authorities*

The provincial/municipal authorities have the responsibility to receive any notifications of planned demonstrations.

They should respond positively to all notifications, unless they are planned on a national holiday or important public day, or if they threaten to do serious harm to national security or cause danger.

If the authorities do not reply within three days – then it should be assumed that there are no objections. If the authorities do object, the organizers of the demonstration have the right to discuss with them and appeal to the Ministry of Interior if necessary.

## *4. The police and security forces*

The police and security forces should protect all peaceful and legal demonstrations. This includes protecting demonstrators from other people who may not agree with their message or cause.

Police and security forces will be responsible for practical steps like closing roads and controlling traffic and helping to keep the demonstration on the agreed route.

If the demonstration becomes violent, or if no notification was given by the demonstrators, the Law on Peaceful Demonstrations gives the police the power to stop and break up the demonstration.

## 5. GROUP FEEDBACK:

- After 15 minutes bring the groups back together and ask each group to present their answers.
- Let the first group present their answers – if they missed anything you should add details from the Suggested Answers above. After this have a few minutes for question and answer, and then move on to the next group.

## 6. DEBRIEF:

- Close the lesson with a short discussion on the new Law on Peaceful Demonstrations. Use these questions to encourage discussion:
  - What do you think about the need to notify authorities about *every* planned demonstration?
  - What do you think about the responsibilities that are put on to the organizers of demonstrations?
  - What do you think about the responsibilities that are put on to the authorities?
  - Do you think that this law will help protect your right to demonstrate, or make it more difficult for you?

### 3. STAYING SAFE AT DEMONSTRATIONS

During a demonstration, organizers and participants can improve their security and the security of others by being well organized. Below are some examples of things that you can do to stay safe:

1. *Know the route* – Make sure everyone knows the planned route and the start and end time of the demonstration.
2. *Know who is participating* – Organizers should know who is demonstrating. As far as possible, have a list of names and contact info for each person participating.
3. *Appoint marshals* – Give some trusted participants the role of "marshal" or observer. Marshals can observe that the demonstration is following the agreed path and that demonstrators are behaving in an appropriate way. If marshals observe a problem they should try and solve it as soon as possible. For example, if some demonstrators leave the agreed route, marshals should explain and bring them back to the proper route.
4. *Cameras* – If possible, try to give some trusted people cameras to document the demonstration. This way you have evidence that the demonstration was peaceful, or if there are problems, you will have evidence of violations.
5. *Plan for dealing with outsiders who cause problems* – Sometimes demonstrations are disrupted by outsiders. If you think this may be a problem, you should have a plan ready for dealing with this. For example, you should inform the authorities as soon as possible that these people are not part of the demonstration.
6. *Identify problems early* – Organizers and marshals may be able to solve problems if they identify them early. If a problem is identified early on it will be much easier to resolve.
7. *Form small groups* – Participants in a demonstration should form small groups within the larger group. This does not mean separate from other demonstrators, you should stay with the main demonstration – but also stay close to your group members. This way, if something happens you will be able to notice very quickly if a member of the group has gotten lost, or been detained or injured. You can then report back to the organizers.
8. *First aid* – If possible, try to have people present that have first aid training and assign a small group to be ready to respond to health and medical emergencies. You could contact an NGO to help you with this. If this is not possible, try to make sure you have basic first aid supplies. Make sure to drink plenty of water if you are out in the sun for long periods of time.

9. *Have a back-up plan* – It is also a good idea to have a back-up plan. If something unpredicted happens, such as very bad weather or the authorities breaking up the demonstration, people should have an alternative place to go to. Make sure that everyone knows where they can go to if there is an unexpected event or emergency.
10. *Think about what you carry with you* – Do not bring any valuable possessions to a demonstration, and never carry anything that some people might see as being a weapon.
11. *Children and youth* – If children and youth are involved in demonstrations, make sure that there is a plan for their security if there is an unexpected problem. If children and youth participate in demonstrations, it is important that they also understand the appropriate way to behave.
12. *NGO Monitors* – You may want to contact NGOs to monitor the demonstration also. This does not mean that they should organize or control the demonstration, but they can be there to observe and record any violations that occur.

## LESSON 2: STAYING SAFE AT DEMONSTRATIONS

**AIM:** Participants will be aware of practical steps that they can take to stay safe at demonstrations.



**MATERIALS:** Whiteboard or flipchart, markers.

**METHOD(S) USED:** Open discussion and brainstorm, role-play.

Procedure	Time Frame (in minutes)
1. Brainstorm	15
2. Introduce the information from Section 1	15
3. Group prepares role-play	15
4. Perform role-play	15
5. Debrief	10
<b>Total:</b>	<b>70</b>

## INSTRUCTIONS TO FACILITATOR

### 1. BRAINSTORM:

- Before you introduce the information from the text, do a short brainstorm session with the group and ask them for ideas on how they think people can stay safe at demonstrations.
- Try to encourage everyone to join in the discussion.

### 2. INTRODUCE INFORMATION FROM SECTION 3:

- Follow the brainstorm by introducing the information from Section 3.
- If some of these points were already suggested by the participants, make sure to acknowledge this.

**Section 3** - It is important that participants understand:

- There are some practical steps that demonstrators and organizers can take in order to increase safety at demonstrations.

### 3. GROUP PREPARES ROLE-PLAY:

- After you have finished discussing the information in Section 3, explain that the group will now use the information they learned in the last two lessons to prepare a short role-play of a demonstration.
- Explain that the participants have the freedom to design the role-play however they like. They can make a well organized and peaceful demonstration with everyone fulfilling their different responsibilities. Or they can show some of the different problems that may happen.
- Tell them to think about the following points:
  - Notifying the authorities
  - Rights and responsibilities of demonstrators
  - Rights and responsibilities of organizers
  - Responsibilities of authorities and security forces
  - Staying safe at a demonstration

- After the role-play, the whole group will have a chance to think about if everyone's rights were respected, and if the demonstrators, organizers and authorities properly fulfilled their responsibilities.
- As the group prepares their role-play, tell them to be thinking about the different practical steps they can take to try to stay safe during a planned demonstration.
- As this is a big role-play with all participants joining in, make sure to provide support and help everyone to be involved in the planning and performance of the role-play.

#### **4. PERFORM ROLE-PLAY:**

- The group performs the role-play.
- At the end of the role-play ask everyone to sit down and ask one volunteer to summarize what happened in the demonstration they created.

#### **5. DEBRIEF:**

- To debrief the lesson, ask participants about what happened in the demonstration they created and whether or not the law was followed appropriately.
- Use the following questions if they are helpful:
  - Was the demonstration peaceful?
  - Did the demonstrators remain within the law?
  - Did the organizers fulfill their obligation under the law?
  - Was the behavior of the authorities appropriate?
  - Did the security forces do a good job?

**DIFFICULT TERMS:**

1. **Demonstration:** When a group of people gather publicly in order to make their opinion known on a political issue or an issue which they feel very strongly about.
2. **Notification:** To give notification means to inform someone about something. In the case of a demonstration, organizers must inform the authorities that a demonstration is planned, what its purpose is, where it will happen, and how long it will last.
3. **Permission:** To ask permission for something means to ask for approval. For example, if you want to build a new building in Phnom Penh, you must ask for permission. Organizers do not need to ask permission to hold a demonstration; they are just required to *notify* the authorities



# YOUR RIGHTS AFTER ARREST

## Outcomes

After completion of this module, participants will:

1. Know what rights people have immediately after arrest.
2. Know what rights people have after they are charged.
3. Understand the right to speedy trial, the right to legal defense and the presumption of innocence.
4. Know different things that they can do if a friend or colleague is arrested.

## 1. ARREST

Around the world it can be seen that people who are active in defending human rights are often arrested or detained by police and other security forces. In some cases this is done without any good legal reason. Because of this, it is important for activists everywhere to understand what their rights are if they are detained, and what duty the State has to protect those rights. It is also important to remember that even if a detained person did break a law, their rights must still be respected and protected.

The Cambodian Constitution states that no one should be arrested for their political beliefs, and no one should be victim of **arbitrary arrest or detention** (arrest or detention without legal reason), however, this still sometime happens.

## 2. RIGHTS IMMEDIATELY AFTER ARREST

Immediately after arrest, and in the hours following, an arrested person has a number of important rights. As stated in the Constitution:

### THE CAMBODIAN CONSTITUTION

Article 38: "The prosecution, arrest, or detention of any person may only be executed in accordance with the law."

This means that no one should be arrested if they have not done anything illegal.

The police may sometimes decide to approach you to ask for information, or even to search you. If the police do not formally arrest you at this stage, there is no obligation to agree to give information or allow the search. However, the police may still decide to arrest you, which means they can take you against your will to the police station. You can only be arrested if:<sup>16</sup>

<sup>16</sup> Code of Criminal Procedure 2008, Article 96.

1. a judge has issued an **arrest warrant** (a court order for your arrest);
2. you are caught in the act of breaking the law; or
3. the police suspect you have committed an offence.

The police can also call you to the police station to answer questions without first arresting you.<sup>17</sup> If you have not been arrested, you have the right *not to attend*, and you have the right to *not answer* these questions. However, if the police think you have failed to cooperate with a police investigation and refused to provide information related to an offence – they may arrest you. Before the police can arrest you for this reason, they must first get an arrest warrant.<sup>18</sup>

If you are arrested or detained, the proper legal procedures must be followed, and your rights must be respected and protected. If you are arrested, these are some of your basic rights:

1. *Right to know why you have been arrested* – The police must tell you immediately why you have been detained.<sup>19</sup>
2. *The police should not hold you for more than 48 hours (two days)* – After 48 hours, you must either be charged or released. The police can hold you for an extra 24 hours if a judge gives permission.<sup>20</sup>
3. *Right to a lawyer* – After 24 hours in custody, you may request to see a lawyer or other person of your choice. If you cannot afford a lawyer, you may want to contact an organization for help.<sup>21</sup>
4. *Right to remain silent* – You have a right to remain silent through the whole process, and no one can force you to speak unless you want to.<sup>22</sup> However, if you choose to remain silent, it may be seen as evidence that you are guilty. Although the law says that everyone should be seen as innocent until proven guilty, this is often not the case in practice.

If you do speak to the police, it is a good idea to wait until you have a lawyer present. If you speak without first talking to a lawyer you may say something or agree to something that harms your case. Sometimes this is not possible, and it can be hard to find a lawyer. If you do decide to speak before you see your lawyer you should be very careful about what you say.

---

<sup>17</sup> Code of Criminal Procedure 2008, Article 93.

<sup>18</sup> Code of Criminal Procedure 2008, Article 96.

<sup>19</sup> Code of Criminal Procedure 2008, Article 97.

<sup>20</sup> Code of Criminal Procedure 2008, Article 96.

<sup>21</sup> Code of Criminal Procedure 2008, Article 98.

<sup>22</sup> Code of Criminal Procedure 2008, Article 143.

5. *Right to be free from bad treatment or abuse* – It is a crime for the police to harm or threaten you while you are in their custody. If you are forced or threatened to confess something, the confession is not valid and should not be used against you in court.<sup>23</sup>



6. *Right to inform your family of your arrest* – If you are under 18 years old, the police must inform your parents or guardian that you have been arrested.<sup>24</sup> If you are under 14 years old, you cannot be detained by the police.<sup>25</sup>
7. *Right to complain if your rights have been violated* – All police and officials with powers to arrest must respect the rights of everyone they detain. If your rights have been violated, you have the right to make an official complaint. These complaints should be resolved according to the law, and the perpetrators punished if guilty.<sup>26</sup>
8. *Innocent until proven guilty* – The presumption of innocence is a basic principle of most legal systems. International law<sup>27</sup> and Cambodian law<sup>28</sup> both state that everyone should be seen as innocent until they are proved guilty in court. This means that an accused person does not have to prove they are innocent, the prosecutor has to prove they are guilty. (The prosecutor works on behalf of the State in a criminal case, and is responsible for the case against the defendant.)

This means that just because someone is arrested or charged they cannot yet be seen as guilty – they must have a trial and the judge must make a decision according to law.

<sup>23</sup> The Constitution of the Kingdom of Cambodia, Article 38; and Code of Criminal Procedure 2008, Article 321.

<sup>24</sup> Code of Criminal Procedure 2008, Article 100.

<sup>25</sup> Code of Criminal Procedure 2008, Article 96.

<sup>26</sup> The Constitution of the Kingdom of Cambodia, Article 39.

<sup>27</sup> International Covenant on Civil and Political Rights, Article 14.

<sup>28</sup> The Constitution of the Kingdom of Cambodia, Article 38.

## SIGNING DOCUMENTS

The police should make a written record of anything you say while you are detained. They will ask you to sign or thumbprint this. You should check this written record carefully, and if it is not correct, you must insist that it is changed before you sign or thumbprint it. The best thing to do is to have your lawyer read anything before you sign it, especially if you have difficulties reading.

*Never sign something that you cannot read.*

If you are forced to sign something you cannot read, and it is later used against you, you should explain to both your lawyer (if you have one), and the prosecutor that you were not able to read the document.

## SEARCHES

Under the law, the police can only search a private residence with the owner's permission or after getting a search warrant from the court.<sup>29</sup>

If you are arrested, your body may be searched by the police and they may confiscate your possessions, but everything should be returned to you when you are released. If you have money, and other possessions like a phone or camera taken from you, try to get a receipt from the officer who takes them.

---

<sup>29</sup> Code of Criminal Procedure 2008, Article 91.

## LESSON 1: YOUR RIGHTS IMMEDIATELY AFTER ARREST

**AIM:** Participants will understand that arbitrary arrest is something that activists face all over the world. They will also know some of the basic rights they are entitled to immediately after arrest.



**MATERIALS:** Whiteboard/flipchart, markers, copies of Handout 1.

**METHOD(S) USED:** Whole group discussion, brainstorming, role-play.

Procedure	Time Frame (in minutes)
1. Introduce the information from Sections 1 & 2	20
2. Explain exercise and divide into groups	5
3. Groups prepare	10
4. Role-play and discussion	20
5. Debrief	5
<b>Total:</b>	<b>60</b>

## INSTRUCTIONS TO FACILITATOR

### 1. INTRODUCE INFORMATION FROM SECTIONS 1 & 2:

- Start the lesson by introducing the information from Sections 1 & 2.

**Sections 1 & 2** - It is important that participants understand:

- Activists all over the world face the threat of arbitrary arrest.
- In Cambodia people have basic rights immediately after arrest, and these must be respected and protected by the police and security forces.

### 2. EXPLAIN EXERCISE AND DIVIDE INTO GROUPS:

- In this exercise participants will be divided into groups. One group will prepare and perform a role play and the other groups will watch the role play and comment on it.
- Divide the participants into groups. Group 1 should have 5 people. This group will perform the role play. Divide the other participants into 4 groups.
- The first group is going to prepare and perform a short role play showing someone being arrested and detained. The other groups will be given a handout with some points to think about. At the end of the performance, each group will talk about the points on their handout.

### 3. GROUPS PREPARE:

- Give Group 1 their handout and tell them to go to one side of the room and prepare their role-play. Explain that they should think about the questions in their handout as they prepare their role-play.
- You may have to help this group to prepare the role-play, especially if they have never experienced or witnessed someone being arrested before.
- Ask the other groups to sit together and discuss the points included in their handouts. Explain that they should think about these points while they watch the role play, and they will have a chance to discuss them afterwards.
- You should make sure that these groups think about their handouts carefully, and be ready to look for these points as they watch the role-play being performed. They should be ready to comment on the role-play and ask questions afterwards.

#### 4. **ROLE-PLAY AND DISCUSSION:**

- After 10 minutes bring the groups together and ask Group 1 to perform their role-play.
- When the role-play is over, choose one of the other groups to discuss the points on their handout. For example, Group 2 should comment on the reasons for the arrest, and if this was in line with the law. Was the person suspected of committing a crime? Was there a warrant for their arrest? Or does it look like the arrest was not legal? They should also comment on whether or not the person was told the reason for their arrest.
- If someone identifies something that was done wrong, they should be able to point out how it should have been done to be in line with the law.

#### **Suggested answers**

The answers will be different depending on what happens in the role-play of Group 1, but below are some important questions that may come up.

- What was the reason for the arrest? Is this a good reason?
- Did the police have an arrest warrant?
- Were they held for the correct amount of time?
- Were they treated well and were their rights respected?
- Were they told the reason for their arrest?
- Did they see a lawyer?
- Were they allowed to stay silent?
- Were they old enough to be arrested and held?

#### 5. **DEBRIEF:**

- To debrief the lesson, do a quick brainstorm of the different rights people have immediately after arrest. Try to involve all the participants and ask them to explain all the rights discussed during the lesson.
- If any important points are missed, you may add them before ending the lesson.

### 3. WHAT CAN YOU DO IF A FRIEND, FAMILY MEMBER OR COLLEAGUE IS ARRESTED?

If a friend or colleague is arrested, there are things that you can do to try to improve their situation. Once someone has been arrested they are under the control of people who are usually much more powerful than them, so it is important to act carefully and if possible work together as a group.

1. *Stay calm* – It is important that you keep calm, even if you are scared or angry. Do your best to keep calm as this way you will be able to think more clearly, react more quickly, and hopefully avoid any further conflict with the police or security forces.
2. *Find out where the person is being held* – It is important to find out where the person is being taken and where they will be held. You can find this out by simply asking the officials who are taking the person away. In some cases the police or security forces may not give an answer to this. In some cases friends, family, neighbors and colleagues have had to followed the police to see where the person was taken.

If no one is around when the person is arrested, visit the area where they were arrested and ask people who were nearby if they saw anything.

Knowing where the person is being detained can make them safer. If you know where they are, you can monitor their situation and you can inform a lawyer or NGO if you need assistance. You may also be able to get information from police officers about why the person has been arrested and what is going to happen to them.



3. *Inform a lawyer* – As soon as possible you should inform a lawyer about the situation. Sometimes this is difficult, so you may need to ask NGO for help.
4. *Inform others* – You may want to inform a respected member of the community, for example, a local official, or community leader who has the trust of local people. In some cases, officials may be sympathetic to your case, so if you have contacts in government you may want to tell them about the situation.

If the arrested person has any medical conditions that you know of, they may need medicines or a visit from a doctor. You should try to explain this to the authorities holding them, as they have a responsibility to protect the health of anyone who is detained.

5. *Solidarity* – If it is clear that the detainees have support from a large number of people, and there is a lot of attention on their situation the authorities are more likely to deal with the case according to the law, and release them if there is no evidence of an offence. It is also less likely that they will be harmed if there is a lot of attention on their case.

## SUPPORTING PEOPLE WHO HAVE BEEN ARRESTED

In 2010, a land dispute started between a community and a powerful business man in a central Cambodian province. The businessman was granted almost 10,000 hectares for a plantation, but the concession overlapped land that was already farmed and occupied by villagers.

Soon after the dispute began, several community leaders were called to the provincial court for questioning. The representatives went to the police station, but more than 400 community members went with them in solidarity.

After several hours of questioning, the representatives were arrested for incitement. Community members stayed at the court and refused to leave until the representatives were released. Around 400 community members stayed outside the court for the rest of the day.

The next day the community members returned to the court and again called for the release of the representatives. Eventually, court officials told the community that if they stopped their demonstration, the representatives would be released the following week. The next week the community representatives were released.

## LESSON 2: WHAT CAN YOU DO IF SOMEONE IS ARRESTED OR DETAINED?

**AIM:** Participants will have the opportunity to share ideas about how to respond if a friend or colleague is arrested or detained.



**MATERIALS:** Whiteboard/flipchart, markers.

**METHOD(S) USED:** Group discussion, sharing session.

Procedure	Time Frame (in minutes)
1. Sharing stories	20
2. Open discussion and brainstorm	30
3. Debrief	10
<b>Total:</b>	<b>60</b>

## **INSTRUCTIONS TO FACILITATOR**

### **1. SHARING STORIES:**

- Start this lesson by asking participants if they would like to share any stories or experiences they have concerning arrest of activists and human rights defenders.
- These stories could be personal, things that have happened to friends or colleagues, or things that people have seen in the media.
- As people share these stories, ask them to think about the rights that were discussed in the previous lesson, and what they think the main problems are in Cambodia regarding rights after arrest.

### **2. OPEN DISCUSSION AND BRAINSTORM:**

- After this sharing session, explain that the class will brainstorm different ways that they could respond if a friend or colleague was arrested.
- Start by explaining that although we discussed in the last lesson that Cambodian and international law protects the rights of people after arrest, there are still problems – and these laws are not always respected. With this in mind, participants should think about different actions they could take if a friend or colleague is arrested.
- Encourage everyone to participate if they have something to say, and ask co-facilitators or volunteers to write down the ideas on flipchart paper or the whiteboard.
- Use the information in Section 3 to add to participants' ideas.

### **3. DEBRIEF:**

- After 30 minutes, debrief the lesson by looking at the answers that participants gave during the brainstorm.
- Return to the stories that people shared at the beginning of the lesson. Ask if any of the actions discussed in the brainstorm were taken in response to the arrests. Were they successful?

**DIFFICULT TERMS:**

1. **Arbitrary arrest or detention:** Arrest or detention without legal reason.
2. **Arrest:** When you are arrested you are formally charged with a criminal offence. At this stage the police can take you against your will to the police station.
3. **Arrest warrant:** An order issued by a court calling for someone's arrest.
4. **Presumption of innocence:** The idea that everyone is innocent until proved guilty in a court of law. In a criminal trial, the prosecution must prove that the defendant is guilty, the defendant does not have to prove that he/she is innocent.
5. **Prosecutor:** The prosecutor works on behalf of the State in a criminal case, and is responsible for the case against the defendant.

### GROUP 1 – ROLE PLAY

Your group's task is to prepare a role play that shows someone being arrested. You will perform this role play for the rest of the group.

Think about these points when you create your role play:

- Why is the person being arrested?
- Where are they being taken?
- What will happen when they get there?
- How long will they be held for?
- Are they questioned?
- Do they get to see a lawyer?
- Are they treated well?

### GROUP 2

1. No one should be arrested without a good legal reason. The police can only arrest someone if:
  - There is a warrant from the court ordering the arrest;
  - They catch the person committing a crime;
  - They suspect the person of committing a crime; or
  - If the person is not cooperating with an investigation.
2. After someone is arrested they have the right to know why they have been arrested.

### GROUP 3

1. The police should not hold someone for more than 48 hours (two days). The police can hold someone for an extra 24 hours, but only if a judge gives permission.
2. After 24 hours in custody everyone has the right to see a lawyer or another person of his/her choice.

**GROUP 4**

1. A detained person has the right to stay silent until they have spoken with a lawyer. He/she cannot be forced to speak, but it may be interpreted as evidence that he/she is guilty by the court.
2. Everyone should be free from abuse and physical harm. It is a crime for the police to harm or threaten someone while they are detained. If someone is threatened or pressured into confessing something, the confession is not valid.

**GROUP 5**

1. If someone is arrested and is under 18 years old, the police must inform the parents or guardian. No one under 14 years old can be detained by the police.
2. All police and officials with powers to arrest must respect the rights of everyone they detain. If someone thinks that his/her rights have been violated, he/she has the right to make an official complaint.



# ANNEX 1: FACTSHEET – INFORMATION SECURITY

## WHAT IS INFORMATION SECURITY?

When we talk about information security, we are talking about keeping your private information safe. This means that the only people that see your private information, or information that you want to keep secret, are the people you choose. When you pass on information to someone else, or when you store information, there is the risk that others may get access to it. There are several things that you can do in order to reduce this risk

## USING THE TELEPHONE

It is very easy for people to monitor telephone conversations and to read your SMS messages. Sometimes it may feel like you have no choice but to talk on the phone, but this may give away sensitive information. There are several practical steps you can take to protect your private information:

1. Always assume that people may be listening in to your conversations.
2. If you want to discuss something very sensitive, you should try to meet and talk face to face with the person you want to discuss the information with.
3. If you cannot avoid using a phone, try and find a public phone or an unregistered phone to make the call.
4. Remember that the person that you are talking to may also be monitored. So the person you are calling should also use an unregistered or public phone.
5. If you can, have a second mobile phone with a different SIM card that is not registered in your name.
6. Do not keep information such as sensitive names and numbers and text messages on your phone. If your phone is lost or stolen, other people can access this information.
7. You may want to use code names for different people or places, this way it will be more difficult for someone to follow and understand your conversation.

## SENDING EMAILS

Emails may be read by people other than those who you send them to. This can happen in two different ways. Firstly, the person you send the email to may forward it or print it and pass the information on to others. Secondly, there is technology that can allow some people to read any emails that you send. This is because when you send an email it goes through the computers of the company who provide the internet service. At this point (and others), emails can be read. Below are a few tips for sending email more securely:

1. Always assume that people may be reading your emails.
2. If you want to discuss something very sensitive, you should try to meet and talk face to face with the person you want to discuss the information with.
3. Try to avoid using sensitive key words. Some programs are set up to catch all emails which use sensitive key words, for example: "demonstration" could be one of these words. Company names may also be sensitive.
4. If you do use email, register for a free email account at somewhere like *Gmail* or *Yahoo!* and when you register, do not use your real name.

Even if the email is private it is better not to say anything that could be considered disinformation, defamation, etc. (Recently one man was charged with defamation for something he said in a private text message.)

## STORING DOCUMENTS

Keeping documentation of your work is important, but it is also important that you keep this information secure. The only people that should be able to see this information should be people who you want to see it. To reduce the risk that others will get access to sensitive documents you can:

1. Store documents in a secure place. This can be in a safe or filing cabinet with a key. You should also lock the room where they are kept if possible. If you do not have access to such a place you should hide documents well.
2. Keep back-up information, copies of computer files and paper files in a secure location.
3. Use strong passwords on your computers and emails. A strong password has a mix of numbers and letters, and uses upper and lower case letters.

4. If you have very sensitive documents and you do not think that you can store them securely, you may want to ask an organization to take care of them for you. However, you must have total trust in this organization, and you must make clear what you want them to do with these documents.

## TALKING TO PEOPLE

When talking directly to people there are also some security risks. Make sure that if you are discussing something sensitive, no one nearby is listening in to you. You should also be careful who you are talking to. Be careful not to give sensitive information to someone if you do not know or trust them. When talking about sensitive topics, think about the following questions:

1. Do you know the person/people that you are talking to?
2. Do you trust the person/people you are talking to?
3. Do they need to know the information you are giving them?
4. Are you in a safe environment to discuss this information?

Likewise, be careful how you speak at meetings, workshops, and other activities.



## ANNEX 2: FACTSHEET – WORKING WITH A LAWYER

### WHAT IS A LAWYER?

Lawyers are people who have received special training in the law and the legal system, and are registered with the *Bar Association of Cambodia*. This special training means lawyers can help people with legal issues by giving legal advice, drafting legal documents and representing them in court. Lawyers can also defend people accused in criminal cases, and try to make sure that their legal rights are protected.

### HOW CAN YOU FIND A LAWYER?

It is sometimes hard to find a lawyer in Cambodia, as there are few lawyers based outside of Phnom Penh and lawyer's fees can often be expensive. In some cases, NGOs may be able to help you find free legal advice.

### WORKING WITH A LAWYER

Working in cooperation with your lawyer is important. Being open and honest with your lawyer about the facts of your case will help him or her to represent you better and make the best arguments for you. Your lawyer has to keep whatever you have told him or her confidential. It is also useful to give your lawyer any documents that support your case.

You should make sure that your lawyer keeps you informed about what is happening with your case. If you have any questions, feel free to ask your lawyer. If your lawyer does not know the answer, he or she should find the answer for you. It is important to remember that your lawyer is working for you, and should put your best interests first. This is especially true if you are paying a fee to the lawyer. You may have to be more patient if you are getting free legal advice from an NGO, as the lawyer may have many cases as well as yours.

### WHEN MIGHT YOU NEED A LAWYER?

There are several different situations where you may want to talk with a lawyer or seek the help or advice of a lawyer. For example:

- You may feel that you want legal advice to make sure that any campaign or action that your group or network has planned is in line with all the relevant laws and regulations.
- If you are arrested you may want a lawyer to come to the police station and be present when you are questioned. If you have been held longer than you should, or if any procedure has been violated, the lawyer may be able to argue for your release.
- If you are called to court it is a good idea to get a lawyer to represent you. If you are charged and called to court, it is your right to have a lawyer represent you. It is better if you can choose the lawyer yourself.
- Outside of court, lawyers can help solve disputes between parties by helping in negotiations.
- A lawyer may be helpful if you need help preparing official documents, such as a request to hold an event.

## RELEASE FORMS

Before a lawyer can represent you, they must have permission from you, usually in a signed document. If you are arrested and people cannot get access to see you, the process of getting a lawyer will be slowed down. Because of this, a number of activists who have received threats or who fear that they may be arrested have already signed forms with NGOs or lawyers. These forms give a lawyer permission to represent them if they are arrested or harmed.

This is only a precaution, and most people will never need to use a lawyer – but in case you are arrested, having signed one of these forms will speed up the process of finding a lawyer and getting legal advice.

If you think you should sign one of these forms you can discuss this further with one of the human rights NGOs listed in Annex 3.

## ANNEX 3: CONTACT LIST

Whether you work as an individual or as part of a group or network, it is important that you take responsibility for your own security planning and precautions. However, there may be times when you need to discuss things with an NGO or ask them for assistance with some activities.

NGOs may be able to help you in an emergency situation, or they may be able to provide you with legal advice, medical care, or monitoring. You may also want an NGO to visit your area and report on your situation, or help set up meetings with officials to discuss your problems.

Remember that if you decide to approach an NGO, you need to be clear what help you would like from them, and that you and other network members remain the key decision makers.

---

*The organizations listed below do not necessarily support the contents of this publication. Their contact details are provided as a resource to access assistance or additional information.*

---

Some of the organizations below have provincial offices. You may be able to visit these offices directly, or get contact details from the numbers provided below.

### **ADHOC**

Address: #1, Street 158, Okhna Troeung Kang, P.O. Box 1024, Beng Raing, Daun Penh, Phnom Penh

Tel: 023 218 653

Email: [adhoc@forum.org.kh](mailto:adhoc@forum.org.kh)

Website: [www.adhoc-chra.org](http://www.adhoc-chra.org)

### **Bridges Across Borders Cambodia (BABC)**

Address: #144-H Street 143, Boeung Keng Kang III, Khan Chamcarmon, Phnom Penh

Tel: 023 220 930

Email: [office@babcbodia.org](mailto:office@babcbodia.org)

Website: [www.babcbodia.org](http://www.babcbodia.org)

### **Community Legal Education Center (CLEC)**

Address: #54, Street 306, Boeung Keng Kang I, Khan Chamkarmon, Phnom Penh

Tel: 023 215 590

Email: [admin@clec.org.kh](mailto:admin@clec.org.kh)

Website: [www.clec.org.kh](http://www.clec.org.kh)

**Cambodian Centre for Human Rights (CCHR)**

Address: #798, St.99, Boueng Trabek, Chamkarmon, Phnom Penh

Tel: 023 726 901

Hotline: 017 50 50 50

Email: [info@cchrcambodia.org](mailto:info@cchrcambodia.org)

Website: <http://www.cchrcambodia.org>

**Cambodian Human Rights Action Committee (CHRAC)**

Address: #9Eo, St. 330, Sangkat Boeung Keng Kang, Phnom Penh

Tel: 023 301 415

Email: [chrac@forum.org.kh](mailto:chrac@forum.org.kh)

Website: [www.chrac.org](http://www.chrac.org)

**Housing Rights Task Force (HRTF)**

Address: c/o CLEC #54, St. 306, Boueng Keng Kang I, Chamkarmon, Phnom Penh

Tel: 023 215 590

Email: [cam.hrtf@gmail.com](mailto:cam.hrtf@gmail.com)

**LICADHO (Cambodian League for the Promotion of Defense of Human Rights)**

Address: #16, Street 99, Boeung Trabek, Phnom Penh. Mailing address: P.O. Box 499, Phnom Penh.

Tel: 023 727 102, 023 364 901

Email: [contact@licadho-cambodia.org](mailto:contact@licadho-cambodia.org)

Website: <http://www.licadho-cambodia.org>

This *Guide to Personal Security for Human Rights Defenders* is a resource for those working in defense of their rights and the rights of their communities. It contains important information about what security is, how to identify security risks, and how to minimize and respond to those risks. The guide also contains information about important laws that impact on the security of human rights defenders.

The guide has been designed and written so that it is accessible to communities, including those who have had limited access to formal education and have little or no prior knowledge of the subject.

The Facilitators' Edition includes interactive activities and instructions for facilitators to run training sessions on each topic.

All across the world, human rights defenders face threats, intimidation, wrongful imprisonment and sometimes violence. This guide is written in a spirit of solidarity and with the aim of supporting those people who risk their lives, freedom and security in order to defend their rights, and the rights of their families, neighbours and communities.

