



Exercises

Prepare
Explore
Strategise

1.1 Exercise

Reflection on existing security practices

Purpose &

Output

This exercise helps you reflect on what security means to you and explore the security tactics, plans and strategies that you consciously or unconsciously have in place.

You get a snapshot of your existing practices, how they interact with each other and how you can use it as a foundation for the next steps.

Input &

Materials

If you want to document the results, write the answers on a flip-chart or sticky notes on a wall.

Format &

Steps

Individual reflection or group discussion

Ask yourself or the group the following questions:

1. Think about the word 'security' or 'safety'. What does it actually mean to you? What do you need in order to feel secure or safe?
2. What do you do every day to avoid danger and protect yourself, your property, your friends or family?
3. When was the last time you did something which made you feel safe and strong?
4. Call to mind an activity you carried out which was dangerous. What did you do in order to stay safe?
5. What other people are important in helping you to feel secure or safe?

6. What resources or activities are important in helping you to feel secure or safe?

Take note of your answers to these questions as they will be useful in later exercises and Sections of the guide and will remind you that you are not building new practices from 'scratch'.

Remarks & Tips	Colleagues or team members might feel strange talking about ‘security’ if there is no existing organisational culture of talking about these issues. This exercise can nevertheless be utilised to start such a process of awareness raising. The exercise itself might start the process of generating ideas on what to improve or add to your security practices. You might want to take notes on these in preparation for Section III Strategise which deals with planning.
---------------------------	---

1.2a

Exercise

Self-awareness exercise: Recognising and reacting to threats

Purpose & Output	The purpose of this exercise is to help you recognise the areas in which your perceptions are most accurate and the areas in which you may be less clear-sighted.
-----------------------------	---

You should gain a clearer understanding of:

- your reactions to threats in the past which went well and not so well
- the gaps in your recognition of threats
- things you may want change
- things which make you confident facing new threats and should be continued.

Input & Materials	Printed copies of the questions
------------------------------	---------------------------------

Format & Steps	Individual reflection Think back on a past experience where you felt particularly unsafe and then acted to take care of yourself. While the experience might have been primarily physical, emotional or related to information security, it might also have had additional impacts on other aspects of your security.
---------------------------	---

**Format &
Steps**

Use the following table to keep track of your insights.

**Remarks &
Tips**

It is helpful to take time for this exercise and write your answers clearly so that you can come back to them as you deepen your self-awareness. If you do this, take care to keep your notes in a private place, sharing your personal thoughts and questions only with people that you trust.

Choose one moment when you felt threatened or in danger and then acted to protect yourself. Consider experiences of physical danger (such as a robbery), emotionally damaging experiences (such as being threatened or betrayed) or threats to your information and communications (such as devices being confiscated or telephones being wire-tapped).

How did you become aware of the threat?

.....

.....

Were there earlier indicators of the threat that you noticed, or maybe failed to notice? Consider indicators in the socio-political environment, in your physical environment, in your devices and in your body and mind.

.....

.....

.....

.....

.....

Were there earlier indicators of the threat that you had noticed, but dismissed as unimportant? Consider indicators in the socio-political environment, in your physical environment, in your devices and in your body and mind.

What were your initial reactions when you became aware of the threat and how effective were these?

What were your subsequent actions and how effective were these?

What would you change if you could go back in time? What would you do instead?

What can you learn from this experience which might help you feel more confident in your ability to cope with future difficulties?

Exercise

Note: If you, your team members, colleagues or fellow activists have gone through traumatic experiences and you want to know how this might impact your perceptions of threats, you can run this deepening exercise. This exercise may be more emotionally challenging so if you do not presently feel ready, consider completing it at another time.

Self-awareness exercise: How traumatic experiences affect our perception

Purpose & Output	The purpose of this exercise is to help you recognise areas in which your perceptions are most accurate and areas in which you might be less clear-sighted due to traumatic experiences.
-----------------------------	--

Input & Materials	It is helpful to take time over these questions and to write down your answers clearly so that you can come back to them over time and as you deepen your self-awareness. If you do this, take care to keep your notes in a private place, sharing your personal thoughts and questions only with people that you trust.
------------------------------	--

Format & Steps	Think back on any past traumatic experiences that may not be fully resolved. These will be experiences that you think about often and which still have the power to make you feel frightened, angry, guilty, ashamed, or sad. Don't go into the actual situation, but focus on what you did to help yourself, what you did to help others and what others did or might have done to help you.
---------------------------	---

Consider the following questions:

- What kinds of dangerous situations are particularly emotionally loaded for you as a result of your past experiences?
- When you find yourself in potentially dangerous environments, are there any situations that make you anxious or scared quite easily?
- Is there someone you trust who could help you identify any unfounded fears you may have?
- What kind of threats do you feel you fail to recognise easily?

**Format &
Steps**

- How might you check whether you are failing to recognise some indicators of danger?
- With whom do you feel comfortable discussing your fears and possible blind spots?

**Remarks &
Tips**

As this exercise might prove to be emotionally challenging, communicate this clearly to your colleagues. It is important that nobody feel coerced into participating in this exercise, and if someone starts to become distressed, they should stop immediately. It might also be a good idea to relate it to other activities, which cover areas of psycho-social well-being.

Optional Exercise: Use of Time¹

As human rights defenders, a very important aspect of our lives which we often lose track of is our use of time. Our workloads are often extremely difficult to manage and our struggle to stay on top of them may come at the cost of our physical and emotional well-being. It may also have a negative effect on our ability to perceive dangers. You can explore this for yourself in the exercise below.

The development of successful security practice demands the commitment of resources, most notably time. As individuals, we need time to reflect on the effect our work is having on us, to ask questions and find answers, to identify successful tactics and tools, to plan and co-ordinate and to integrate new practices into our lives and work.

Feelings of emotional security are often related to our use and perception of time. What is the ratio between our working or engagement hours and the time we spend with our loved ones or for recreational activities? As activists, we nearly always face the dilemma that our workload never ends but our energies do. So where do we draw the line? The “Use of Time” exercise from the Integrated Security Manual helps us to make conscious steps towards a healthier and more emotionally secure use of time, which you can find in **Appendix E**.

¹ Reproduced from Barry, J. (2011) Integrated Security: The Manual, Kvinna till Kvinna Foundation, Stockholm.

Talking about security in groups and teams

Purpose & Output The purpose of this exercise is to reflect on how and when we talk about security with our peers, colleagues or team. It is best facilitated by at least two people, but can also serve as a useful individual reflection on your interaction with your colleagues. This helps start a process to constructively talking and discussing security in your team / group.

Input & Materials To do this exercise in a participative way and in order to document it, you may need writing material (cards or stickies and markers). A large area of wall-space, a flip-chart or pin-board may also be useful.

Format & Steps **Individual work & group discussion**

Step 1: Divide the group into pairs. Ask each pair to consider the following questions concerning group dynamics and write down their answers.

- What topics take up the majority of time in group conversations?
- What topics do we never seem to find time for? What aspects of our group interaction do we find energising?
- What aspects of our group interaction do we find exhausting?
- What happens in the group when people disagree?
- Have you created any space to develop and refine your own security practices (as an individual)? Describe it: where and when does this space exist? Is it sufficient, and how might you expand this space, if necessary?
- Do you have enough space to talk about security issues with others, such as peers or colleagues who work closely with you, and how might this space be created or expanded if necessary?

**Format &
Steps**

Step 2: Collate the full set of responses to these questions on a board or in a notebook.

Step 3: As a team, consider the following questions.

- Where and how do we want to set our priorities concerning security?
- What are common problems that arise around talking about security as a group?
- What can prevent us from talking about security? How can we deal with this?
- How can we create and maintain sufficient and adequate space for talking about security? What will this mean in terms of time and resources?
- How might we increase the effectiveness of our group interaction on security?
- What problems arise around committing to changing our security practices? Do we resist change, individually or collectively, and why?

Step 4: Invite each person individually to reflect on:

- Whether you should have a similar awareness for your family and loved ones?
- What are the differences in the dynamics and ways in which family and loved ones are affected?
- In what ways do you communicate the threats you are facing to your family, community, friends and others not in your work circle?

Step 5: In the whole group, share the points that people feel free to share. Then you should agree on what can be communicated to those ‘outside’ the group, for reasons of confidentiality, intimacy and security. Agree on these guidelines for the whole group.

**Remarks &
Tips**

Consider also discussing the steps and requirements necessary to put your ideas of how to talk about security in the future into practice.

Remarks & Tips	<p>Important questions to consider might be:</p> <ul style="list-style-type: none"> • What happens if you don't progress on 'talking about security'? • What happens if someone does not stick to the guidelines on what can be communicated to the outside?
---------------------------	--

1.5b

Exercise

Non-violent feedback

Purpose & Output	<p>The purpose of this exercise is to practice non-violent communication as a means of improving the effectiveness of communication about security within teams and groups. It provides for a reflection on how we can give our feedback in an understandable, clear way and avoid some of the pitfalls which can lead to arguments or ineffective communication.</p> <p>The exercise is best carried out in pairs at first, although it can be adapted for larger groups.</p>
-----------------------------	--

Input & Materials	<p>It may be useful to write the guidelines for non-violent feedback somewhere visible, like on a flip-chart.</p>
------------------------------	---

Format & Steps	<p>Decide on a setting for conducting a feedback discussion (this can be done in pairs, or with observers, taking turns). The participants should choose a topic (real or imaginary) about which they want to give feedback. This can be a security-related topic, such as an incident which took place already, or something else entirely.</p> <p>Ask the person giving feedback to follow the guidelines below. For each guideline, a small illustrative example is given. Here, we are imagining a scenario in which two colleagues are talking: one of the colleagues often works late and once forgot to lock the door of the office when leaving; the other colleague wants to talk about the incident.</p>
---------------------------	--

Format & Steps

The recipient of the feedback should only ask questions of clarification but not comment, reply, justify or question the content of the feedback.

Guidelines for non-violent feedback:

I speak for myself: You can only speak from your own subjective experience – not about ‘common sense’, ‘my group’, ‘we’, or ‘one’, but only ‘I’.

- e.g. “I felt unsafe when I found the office unlocked this morning”.
- Bad practice: “What you did yesterday put us in danger!”

What did you observe? You should speak only of the facts as you experienced them, so the interlocutor knows what your feedback is referring to (what you saw, heard, etc.).

- e.g.: “When I arrived at the office this morning, the front door was unlocked and I could open it without the key”.
- Bad practice: “You forgot to lock the door yesterday!”

What was your reaction to it? What were your internal feelings and physical reaction to your experience? Try not to be judgemental, but again, simply speak from your experience as you understand it.

- e.g. “I was very worried, because I thought maybe we had been robbed. When I found that everything was OK, I was still quite angry.”

How do you interpret it? What does your personal interpretation bring to the facts? Although your personal interpretation is indeed subjective, it is still valuable and colours your experience.

- e.g. “I think it happened because you have been working very late and were tired and simply forgot to close it”

What are your wishes, advice, or interests? What are your suggestions for change based on this experience? They should be offered without demands, but rather as requests for consideration by the group.

- e.g. “I would feel better if I knew we were all getting enough rest and not overworking so that we could better take care of things like this, so it would be better if you didn’t work so late”.

**Format &
Steps**

Ask the pairs to then share their insights on the process and manner of giving feedback – not about the content. Did they experience different feelings than when they normally receive feedback?

This exercise can also be used to clarify the content and tone of your feedback as a preparation for an actual feedback session or potentially difficult discussion.

**Remarks &
Tips**

It is important to receive feedback with your ears and not with your mouth, and understand it as a personal reflection from your partner, not as ‘the truth’ or an invitation to justify or defend your actions. You decide yourself if it is valuable to you and how to react to it. Following such an approach might be a preventive step for conflicts within your team. As such, it can contribute to your overall well-being.

If you are interested in deepening modes of communication which deal sensitively with conflict, you might want to have a look at non-violent communication approaches.

Be aware that ‘speaking for myself only’ is not appropriate in many regions around the world. Adapt the methodology so that it fits your needs and setting.

Situational monitoring: quick PESTLE analysis

Purpose & Output This exercise helps us consider the ways in which we already carry out a situational analysis, and briefly consider some of the dominant trends and developments in the last 12 months which may impact our security.

Input & Materials Writing materials

Format & Steps Alone or in a group, consider and take notes of your answers to the following questions:

1. How do you currently carry out situational monitoring and analysis? What spaces do you have for discussing ongoing developments in society?
2. What are your sources of information for this?
 - Make a list of these, and for each one, take notes on their strengths and weaknesses in terms of the quality of information they offer. Are they objective or biased?
3. Consider what has happened locally, regionally and internationally in the last 12 months and make a list of 5 to 10 developments you consider important. You may not need to categorise them, but be sure to consider:
 - political developments
 - economic developments
 - social developments
 - technological developments
 - legal developments
 - environmental developments.

**Format &
Steps**

Note: If you can't think of new developments in the last 12 months, consider generally salient characteristics.

4. Could any of these developments impact your security, directly or indirectly? If so, how? Did you suffer any attacks or accidents in the last year? How did they relate to these developments?
-

2.3a

Exercise

Visual actor mapping – part 1

**Purpose &
Output**

The idea of this exercise is to begin a process of visualising yourself, your group or organisation, and your relationships to the other actors around you, including direct, indirect and potential future connections.

In this part, we suggest that you focus on brainstorming who the actors around you are and the intensity of your relationship with them (direct, indirect, or potential).

In the next step of the exercise, you will extend the visualisation or map to include the types of relationship you have with them.

**Input &
Materials**

If you want to carry out this activity in a group, you will need:

- butcher-block or flip-chart paper
 - coloured markers or pens
 - sticky-notes / Post-its.
-

**Format &
Steps**

Written/drawn visualisation

In this exercise we suggest that you use sticky-notes or post-its, each with the name of one actor in your context, to visually map them and the relationships between them.

1. Start with yourself or your organisation as an entity and brainstorm and identify as many actors related to your work as possible. This can include individuals, groups, organisations or institutions. Consider local, regional, national and international actors where necessary.

Format & Steps

2. Once you have identified as many of the actors as you can, place them on the wall or sheet, with yourself (and/or your target group, if they are identifiable) in the centre.
3. Consider the following categorisations for these actors:
Direct: People, groups, organisations, institutions that have direct contact with you on the issue you are trying to impact. For example, you probably have a direct relationship to the target-group you work for, and some entities directly opposed to your work who directly challenge or confront you.

You may also want to include members of the community around you including your family and friends who may support or oppose your work in one way or another.

- **Indirect:** These can include people, groups, organisations or institutions that are one step removed from you. In the example above, if your target group has a direct relationship with you, they may be in direct relationship with others. These become indirectly connected to you.
- **Potential/Peripheral:** People, groups, organisations and institutions which relate to the issue, but with whom you don't (yet) have a connection or relationship. Examples of these include international bodies which are supportive of your issue, but aren't (yet) active in your context.

Note: Actors and information

Although it may not have occurred to you, you may want to include actors on whom you rely to manage your information and communication. These can include:

- your telephone service provider
- your internet service provider
- social media account providers
- email account providers.

We will explore these actors in more detail in the next exercise.

Remarks & Tips

In the next and subsequent Chapters, we will expand our knowledge of these actors and use them to build our analysis of threats. Once you have finished this exercise, it's a good idea to keep a list of these actors for future reference and elaboration.

Visual actor mapping—part 2

Purpose & Output This exercise builds on [Exercise 2.3a](#) by denoting relationships among the actors in the map, identifying the allies, opponents, and neutral parties.

The resulting map can then be used to identify and analyse specific actors in your context who may represent intentional (or unintentional) sources of threats.

Input & Materials

- A basic actor map (from the previous exercise)
- Paper and coloured markers or pens
- Coloured dot stickers

Format & Steps **Written/drawn visualisation**

Considering all the actors you have brainstormed so far:

1. Denote actors based on the nature of their relationship to your work (ally, adversary, neutral, unknown). This can be done by assigning a coloured dot to each type of actor, different coloured post-it notes, or different locations (allies on the left, opponents on the right, neutrals in the middle, etc.).
2. Draw a circle around each actor on the map. Its size can correspond to its **power and resources** in the socio-political context (see legend below).
3. Starting with yourself on the map, you can make connections to any actor with whom you have a relationship.

Use the legend on the next page to represent the different types of relationships that exist between the actors on the map.

Examples of relationships to include here are:

- Close relationships: where actors enjoy a positive relationship with each other.
- Alliances: where actors coordinate their activities with one another and act as one.

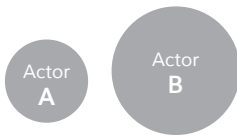
Format & Steps

- Weak or unknown relationships: relationships with little contact, or where the nature of which is unknown.
- Conflict: where two actors have an antagonistic relationship with one another.
- Violent conflict: where the relationship is characterised by physical (potentially armed) violence by one or both parties.
- Compulsion: where an actor has power over another one and can make them do something, e.g. a paramilitary group which is controlled by the armed forces.
- Interdependent: where two entities are bound to each other in some manner.

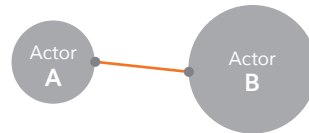
Remarks & Tips

It is useful to periodically revisit and reflect on the map you created and make any additions, subtractions or changes that occur to you. Remember, it is important that this is re-evaluated and updated regularly, especially before a new action.

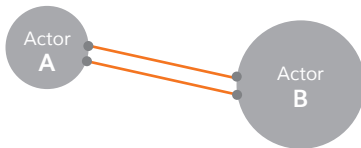
Legend²



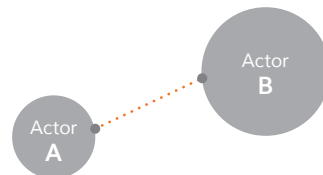
Different sized circles represent differences in power



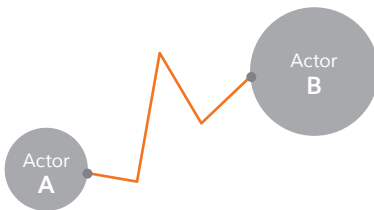
A solid line represents a close relationship
You can also 'break' the line (by crossing it in the middle) if there is a broken relationship



A double-line represents an alliance



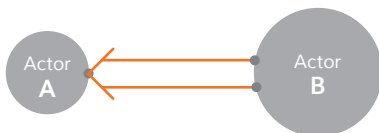
A dotted line represents a weak or unknown relationship



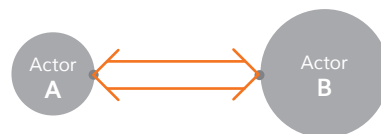
A jagged line represents conflict or a bad relationship



A double jagged line represents violent conflict



A double-line with an arrow represents domination, control or compulsion (where one actor acts under orders of another)



A double-line with an arrow in both directions represents interdependence

² Adapted from KURVE Wustrow (2006) Nonviolent Conflict Transformation. A Training Manual for a Training of Trainers Course. Centre for Training and Networking on Nonviolent Action KURVE Wustrow e.V., Wustrow. (pdf: <http://www.trainingoftrainers.org/>), pp.45-46.

Additional actor information sheet

For each of the allies and opponents (but prioritising the active ones), you can elaborate on the nature of their relationship to your work, and create an information sheet that provides further information on their motivations, their interests, the history of their relationship with you and their resources (material, financial, relational or other).

This information sheet will help you to:

- identify the underlying interests and relationships that motivate their stance. Why are they 'with' or 'against' you?
- identify the resources and strategies they possess and employ which they may use to help or hinder your work. Reflect also on their position within the broader socio-political context and which privileges and resources they might draw from that position.

It is important to note that these motivations and resources will change over time. This analysis should be updated regularly as new information emerges. Furthermore, it's very important to consider sources of information about this trustworthy: be it through personal contact, informal networks, local media or other.

2.4 Exercise

Information ecosystem

Purpose & Output The purpose of this exercise is to take an inventory of the most important information assets you manage, in order to create policies for its safekeeping later on.

Input & Materials It may be helpful to reproduce the example table below, either by printing it or drawing it on a flip-chart or other materials.

Format & Steps **Brainstorming and documentation**

To begin the exercise—especially in a group—it may be useful to use a spreadsheet, or a large sheet and sticky notes, or some other means which allow you to brainstorm easily and group things together.

Brainstorm and make a list of all of the data you manage. If you're not sure where to begin, consider:

- data related to each of your human rights activities
- personal data and files, especially if stored on your work computer
- browsing activities online, especially of sensitive data
- emails, text messages and other communication related to your human rights activities.

Imagine a spreadsheet that has several columns enumerating categories as described below. Your task is to fill the rows with information.

Start with your information at rest, and for each type of information, elaborate on the following

- what information is it?
- where does it reside?
- who has access to it?

Format & Steps

- how sensitive is it?
 - secret
 - confidential
 - public
- how important is it to keep it?
- who has access to it?
- how should it be protected?
- how long should it be kept before destroyed?

Characterise and qualify the information you have mapped out. You can repeat the same process and expand the spreadsheet with additional entries for your information in motion; e.g. data being transferred (physically, electronically), communications over the internet or telecommunications networks.

The questions and example in [Table 2](#) below may help you with this.

Remarks & Tips

This process is iterative. Once you have done the first round, you may detect patterns and groupings. For instance, you may decide that since all financial information (regardless of type) has similar sensitivities and longevity, you can group them and think of them as a financial information category.

Conversely, you might find yourself needing to expand a row into several rows. For instance, a row containing 'email' needs to be expanded to several rows to account for a subset of emails – and their safe-keeping – which is sensitive.

This should be a live document and will change according to shifts and developments in your situation. So you will benefit from regularly updating this document to account for any of these changes.

Table 1.

Information at rest				
What (examples)	Attributes			
	Where does it reside?	Who can/does access it?	How sensitive is it?	How should it be protected?
Financial documents in electronic form	Secure shared folder – file server	Executive team	Secret	Saved in hidden encrypted partition. Backed up daily to encrypted hard-drive
Program reports for the censorship campaign	Documents folder – file server	Team members, program director	Confidential	Saved in encrypted partition
Adobe InDesign for the web developer	Web content manager's laptop	Web content manager	Confidential	Licensed, password-protected

Table 2.

Information in motion					
What (examples)	Attributes				
	What method of transfer are you using?	Who has (or wants) access to it?	What physi- cal or virtual routes does it take (origin, path, destination)?	How sensi- tive is it?	How should it be protected?
General emails among team members	Email (Gmail)	Team mem- bers, email provider	Origin: staff computers Path: internet (via Google servers) Destination: staff computers	Confidential	GPG encryption
Check-ins during missions	Text messages (SMS)	Team members, telecom company	Origin: mobile phone Path: mobile network Destination: mobile phone	Secret	Code words

Security indicators in our daily life

Purpose & Output The purpose of this exercise is to help us get an overview of our daily routines and other activities, through visualising it and noting the points at which we can check for indications of a change in our security situation.

We can use this overview of our routines to make a check-list of moments in the day where we can establish a base-line and subsequently check for potential security incidents.

Input & Materials Use whatever drawing materials you would ordinarily use, and either a notebook, electronic document, whiteboard, etc. for creating your check-list.

Format & Steps **Visualisation: Drawing, writing**
In this exercise, we suggest that you use drawing as a way of visualising your routines. Although drawing may seem strange at first, it is a useful way to externalise your routines to get a different perspective on activities you may normally not consider from the perspective of security.

Draw a typical working day, or a day during which you are carrying out an activity you consider dangerous.

Do not worry about making it too visually accurate or artistic: just enough for you to understand it yourself. Simply begin with where you are when you wake up in the morning and consider things like:

- Where you are when you have breakfast, if you have breakfast?
- If you work outside of home, how do you get there? In what vehicle, with whom, and via which areas?
- When you go to work, what devices do you bring with you? What other things do you bring (keys, wallet...)?
- Where do you work, and who else is there? How do you work and what devices do you use for that?

Format & Steps

- If you eat lunch or dinner during work, include this. How long do you give yourself and where do you eat?
- What time do you stop working? If you work away from home, how do you get home? What route do you take?
- What do you do before you sleep? What time do you normally sleep?
- Where do you regularly spend time apart from work and home?

Once you have a picture of your day, try to look for moments where you may want to stop and establish a 'baseline', i.e. what a normal day looks like in order to later check for signs that anything unusual is happening in your physical surroundings. Some suggestions might include:

- The vehicle in which you travel: are there any signs of tampering (wheels, brakes, steering, ...)?
- The route you take to work: are any of these areas dangerous? Is it worth checking whether you are being followed?
- Your office or workspace: is everything in its place when you arrive, and before you leave? Are the doors and windows locked?
- The space immediately around your home or office: is there anyone or anything (for example, strangers, police or vehicles) out of the ordinary here?

Note down the moments when you will check for signs of danger in your physical surroundings, and consider sharing them with trusted friends, neighbours and colleagues. If you consider yourself at high risk, you might include the daily routines of your family members or other close persons.

Create a check list from the results: what will you check, and when?

Remarks & Tips	<p>Going through this process is meant to help identify both instances when we carry out an action or take a precaution based on our own sense of security, as well as to notice moments when we may feel a need to pay more attention or take precautions.</p> <p>If you carry out many diverse activities in your human rights work, try to repeat this exercise for the different ways in which you work.</p> <p>The purpose of sharing this with a trusted friend or colleague is to make ensure we double-check and confirm our observations and/or cover potential areas we may have overlooked.</p>
---------------------------	--

2.5b

Exercise

The stress table

Purpose & Output	<p>This exercise can help you to identify your limits concerning different kinds of stress, how to recognise these limits and measures to counter stress. Take some time, ideally when you are not under stress and try to create your own stress table.</p>
Input & Materials	<p>For this exercise we differentiate between three levels of stress, like a traffic light:</p> <p>Green = bearable, motivating stress. This kind of stress might keep us creative, but we may become tired more easily, need more breaks and know that we don't want to feel it for a long period of time.</p> <p>Yellow = unpleasant stress. With this level of stress, we may feel tired and at the same time alert. We may manifest physical signs of stress (which vary from person to person). We will usually have a strong desire to change the situation which is causing this sensation.</p> <p>Red = unbearable, profound and lasting stress. This kind of stress affects different spheres of our lives including our relationships at work, with our friends and family as well as</p>

**Input &
Materials**

our personal relationships. This level of stress also reduces the pleasure and relaxation we take from recreational activities, and we feel anxious and/or miserable. Our bodies show clear physical reactions, and we may feel close to collapse, and resort to unhealthy measures to stay alert, such as stimulants.

**Format &
Steps**

- Step 1:** Basing yourself in the example below, draw up an initial stress table and reflect on it with somebody you trust.
- Step 2:** Decide on a regular schedule, when you want to review your stress status, and try to carry out these reviews accordingly.
- Step 3:** If you frequently experience high stress levels over a period of time, review your stress table to determine if it is still adequate.
-

**Remarks &
Tips**

Checking this stress table could be one step in your personal security guidelines and should be done regularly. Be sure to check if your definitions for the different levels are still accurate, or if you have simply become accustomed to higher stress levels!

	Indicators (How do you recognise that you are at this stress level? What makes this phase qualitatively different from the previous level?)	What can you do to reduce the level of stress, or increase your ability to cope?	Resources needed
Green
Yellow
Red

Bear in mind that emotional dangers are sometimes subtle and can creep up on us. They increase slowly over time and we may fail to notice how much has changed. Some strategies for regularly scanning for indicators of emotional danger include:

- paying attention when friends and family comment on your mood, appearance or interpersonal behaviour
- actively seeking out feedback from trusted friends and colleagues who care about you enough to be truthful with you
- keeping a private diary of your thoughts and feelings from day to day
- paying attention to ways in which your stress level might be making you less aware of security indicators (physical, informational, or emotional) in your environment;
- if necessary, seeking advice and support from a mental health professional.

Threat brainstorm

Purpose & Output This exercise is a first attempt at identifying the threats to yourself, your group or organisation and your work in defence of human rights. This initial list of threats can then be refined so as to focus in more depth on the threats which are most likely or potentially most harmful.

Input & Materials Inputs: this exercise will be easier if you start with:

- your analysis of the ongoing political, economic, social and technological trends in your context
- a list of the activities or types of work you carry out in order to achieve your objectives
- your actor map, particularly the opponents
- a list of security indicators you have observed in your previous work.

Suggested materials:

- **If alone:** a sheet of paper or some other materials for writing.
 - **If in a group:** a large sheet or flip-chart and writing material.
-

Format & Steps Consider and write down all the potential threats to yourself, your organisation and your work. It may be helpful to categorise them beginning from each of your activities or areas of work. Remember: a threat is any potential event which could cause harm to ourselves or our work. Don't forget to consider potential threats to your information security and threats to your well-being, political or otherwise.

Create a list of these threats. If you find it difficult, consider your opponents and the ways in which they have acted against other human rights defenders in the past. Analyse your security indicators and consider whether they represent a concrete threat.

**Format &
Steps**

Observe any patterns that emerge in the threats you identified: do they relate primarily to certain activities of yours, or originate from certain opponents? This will be useful when it comes to security planning (i.e. by planning particularly for certain activities, or dedicated plans for engagement with some actors).
Keep this list for analysis in the following exercises.

**Remarks &
Tips**

If the list is somewhat long, it may be overwhelming to consider these potential threats. It may also be a challenging exercise as we may not know how realistic we are being.
It's important to remember that political threats always originate from a certain actor or set of actors who see their interests potentially threatened by you and your work. In a sense, threats are a sign that your work is effective and that your opponents fear your work. While it may be a moment which inspires fear, clearly recognising the threats you face should also be a moment of empowerment. Acknowledging these threats and the likelihood of their occurrence allows you to better plan for and potentially mitigate the damage caused to you or your work, should one of them occur.

Reflection on perceiving threats

Purpose & Output Improving the recognition and analysis of threats in order to respond adequately.
You will learn to recognise your own blind spots and missing processes for identifying threats as well as creating processes to fill these gaps.

Input & Materials Use the list of threats from the threat brainstorm ([Exercise 2.6a](#)) for this exercise.

Format & Steps Individual reflection or group discussion

Ask yourself or the group the following questions:

1. Were there any threats which you discovered or which were mentioned by others, which you wouldn't have been aware of previously?
 2. If you did the exercise in a group, was anyone else surprised by the threats you mentioned? Why?
 3. How long do you think the threats you identified existed before you became aware of them?
 4. How might you have become aware of them sooner?
 5. How do you communicate in your group, with your colleagues about them?
 6. What makes them feel more or less serious?
 7. Can you identify any threats that feel more serious than they might actually be?
 8. If you are working with a group: what are the differences in your answers to the above? What makes you think of the same threat in different ways?
-

Remarks & Tips	It can be overwhelming listing all the threats you face. Be sure not to rush this exercise and to allow space for people to express their feelings as they go. If you find this exercise useful, consider making it a regular (weekly or monthly) exercise.
---------------------------	---

2.6c

Exercise

Threat inventory

Purpose & Output

This exercise will help you prioritise threats and divine the causes, ramifications, sources as well as the required resources, existing actions and possible next steps.

The output of this exercise is an inventory of your prioritised threats in some detail, which will be used in the next Chapter to help you create plans of action.

Input & Materials

- Actor and relational maps
- Information ecosystem
- Security indicators
- Impact/likelihood matrix

- Pens and paper
- Flip-chart
- Markers

Format & Steps

First, beginning with the threat brainstorm from the previous exercise, consider the threats listed in terms of their likelihood and impact. Make a selection of those you consider to be most likely and as having the strongest impact to use for the next exercise.

Again, it may be useful to separate and organise threats according to particular activities (e.g. separating those which specifically arise in the context of protests from those which relate to the day-to-day running of your office).

Format & Steps

Start with what you consider the highest priority threat, based on the impact/likelihood matrix, and using the example template provided, elaborate (individually or in a group).

- Write down the title and summary of the threats.
For each threat, if it is a complex threat, you may decide to divide and analyse sub-threats (for instance, an office raid and arrest may be easier to analyse if separated to include the numerous consequences each would include – potentially arrests, confiscation of devices, judicial harassment, etc.). Use the rows to expand each of the below per sub-threat.

Work through the following questions for each threat. It is possible that some threats are complex, and some of the answers require their own space. Use as many rows as necessary. If, for instance, a threat constitutes an attack on a person, as well as the information they are carrying, you may want to use one row to describe the informational aspects and another for the person in question.

- **What:** Describe what happens if the threat is carried out. Think of the impact it might have on you, your organisation, your allies. Include damages to physical space, human stress and trauma, informational compromise, etc.
- **Who:** Identify the person/organisation/entity behind the threat: Referring back to the actor map, you can focus on information regarding this specific adversary:
 - What are their capabilities?
 - What are their limitations to carrying out these threats?
 - Are there neutral parties or allies that can influence them?
 - Is there a history of such action against you or an ally?
- **Who/what:** identify the potential target of the threat; specific information being stolen, a specific person under attack (physically, emotionally, financially), material and resource under threat (confiscation or destruction of property).
- **How:** What information is needed?
 - What information is necessary for the adversary to be able to carry out the threat?
 - Where might they get this information?

Format & Steps

- **Where:** describe the place where the potential attack might take place.
 - Does an attacker need access to the same location as you, as is often the case in a physical attack?
 - What are the characteristics of the location in question? How can we you it to keep safe? What is more dangerous about it?

Elaborate on the psychological, emotional and health factors as they relate to this threat, including the effect your stress levels, tiredness, fear and other factors on the potential occurrence of this threat. Consider:

- How might your current mindset affect any planning and contingency measures being carried out?
 - Does this threat take place in the context of a particular activity? What kind of mental or physical state do you find yourself in during such activities? What are some best practices which may protect you, or what might make you more vulnerable?
 - What elements of your behaviour or state of mind may actually increase the probability of this happening, or its impact?
-

If you wish to record the results of the exercise in writing, you could use a format like the one below:

Threat	[Title of the threat]			
Summary	[Brief description/summary of the threat]			
What	Target	Adversary	How	Where
Describe what happens if the threat is carried out (if required, subdivide the threat into its components below).	Specify what/who is the target.	Who is the entity behind this threat?	What information is necessary to carry out the threat?	What are physical spaces in which the threat can manifest?
1)				
2)				
3)				
Psychological, emotional and health impacts				

Existing practices and capacities

Purpose & Output In this exercise, you can consider each of the threats you already identified and prioritised in light of your existing security practices and other capacities relative to them. This will give you a ‘baseline’ on which you can later build and improve.

Input & Materials To carry out this exercise, you need to have identified and prioritised threats in [Exercise 2.6b/c](#). It may be helpful to write out the the capacities you identify so you can review them later.

Format & Steps Return to the threats identified in [Exercise 2.6b](#). For each of the threats you have identified, there were a series of questions. Here you can relate your existing security practices and capacities to each of these questions as follows:

- **Who/what** is under threat? Identify here what capacities (if any) are already protecting this person or thing from this threat. Examples of capacities could include
 - in the case of judicial harassment: good legal knowledge
 - in the case of computer confiscation: having encrypted hard drives.
- **Who** is behind the threat? Do you already have some kind of tactic for engaging with this actor? Are there any tactics or resources you have leveraged in order to prevent them from acting against you? If so, what? If they have acted against you before, did you respond in some way? If so, how? If you don’t have any, that is fine: this will be important to remember when you identify gaps.
- **How**: What information is necessary for them to carry out the attack? Do you have any information protection or counter-surveillance practices in place which might prevent that information from falling into their hands?

Format & Steps

- **Where:** What access to you or your property do they need? How do you secure the physical spaces around you (e.g. buildings, vehicles, private property) in order to protect yourself and your property? For example, do you lock your offices and homes? What ‘common sense’ practices do you have for your personal safety in dangerous environments? All of these are important to note, so that you don’t start from zero!
- **Psychological, emotional and health tactics:** Include any well-being practices that are in place to deal with this threat – do you have any practices which help to reduce stress, tiredness etc., and increase centredness and awareness which may help respond to this threat?

Where possible, try to consider these aspects relative to each of the threats you have identified. **If you can’t think of an answer for one or more of the questions, that is fine:** you have just identified a gap to be filled! You will consider gaps in the following exercise, and use them as a way to identify what new resources and practices you need.

Remarks & Tips

Caution! For each of the answers you give, consider **whether this practice or capacity is positive. How do you know?** There is a slight danger of creating a false sense of security if you falsely credit an existing practice with helping to keep you safe. If you are not sure about something, it would be worth taking the time to think over and **talk to your colleagues or trusted friends** in order to get a fresh perspective.

If you wish to record the results of the exercise in writing, you could use a format like the one below:

Threat	[Title of the threat]			
Summary	[Brief description/summary of the threat]			
What	Target	Adversary	How	Where
Describe what happens if the threat is carried out (if required, subdivide the threat into its components below).	Specify what/who is the target.	Who is the entity behind this threat?	What information is necessary to carry out the threat?	What are physical spaces in which the threat can manifest?
1)				
2)				
3)				
Psychological, emotional and health impacts				

Vulnerabilities and gaps in our existing practices

Purpose & Output In this exercise, you can consider each of the threats you identified and prioritised in the previous Section, Explore, in light of the gaps in your existing security practices and your vulnerabilities. This will give a much clearer picture of where you need to begin building new capacities.

Input & Materials To carry out this exercise, you need to a) have identified and prioritised threats in [Exercise 2.6b](#), and b) collated the output from [Exercise 3.1a](#) above.
Use pens and paper or other writing materials.

Format & Steps Return to the threats identified in [Exercise 2.6b](#) and the existing capacities and practices you identified in [Exercise 3.1a](#). Here, you can attempt to identify the gaps in your existing practices and your vulnerabilities, relative to each of the questions you answered previously. Consider the following questions:

- **Who/what** is under threat? Identify here what gaps or vulnerabilities (if any) are making this person or thing more vulnerable to the threat. Vulnerabilities could include:
 - in the case of judicial harassment, a person having little legal knowledge, or
 - in the case of computer confiscation, the hard-drives having no password or disk encryption.
- **Who** is behind the threat? What vulnerabilities or gaps exist in our ability to influence this actor? For example, if there is no way of directly engaging with the actor to create acceptance of your work or deter an attack, this could be considered a gap.
- **How**: What information is necessary for them to carry out the attack?
- Is it difficult to control the flow of information – are there any vulnerabilities in the way you deal with information relevant to your work that may facilitate this threat or make it more damaging?

Format & Steps

- **Where:** What aspects of the physical spaces around us (e.g. buildings, vehicles, private property) may make this threat more probable or more damaging? In the case of an office raid and theft, for example, having weak locks on the doors would be a vulnerability.
- **Psychological, emotional and health vulnerabilities:** in the context of this threat, how might stress, tiredness etc. affect you? What gaps or vulnerabilities exist in your well-being practices that may make this threat more likely, or more damaging?

If you wish to record the results of the exercise in writing, you could use a format like the one below:

Threat	[Title of the threat]			
Summary	[Brief description/summary of the threat]			
What	Target	Adversary	How	Where
Describe what happens if the threat is carried out (if required, subdivide the threat into its components below).	Specify what/who is the target.	Who is the entity behind this threat?	What information is necessary to carry out the threat?	What are physical spaces in which the threat can manifest?
1)				
2)				
3)				
Psychological, emotional and health impacts				

Brainstorming new capacities

Purpose & Output In this exercise, you can consider each of the threats you identified and prioritised in [Section II | Explore](#), your capacities and your vulnerabilities in order to identify the new capacities you need to build in order to maintain your well-being in action.

Input & Materials To carry out this exercise, you need to have identified and prioritised threats in [Exercise 2.6b](#), and the outputs from [Exercises 3.1a](#) and [3.1b](#) above.

Format & Steps Reflect on the threats you face and your existing capacities and vulnerabilities identified in the previous exercises. You may want to write down your answers on a format such as the one in [Appendix D](#).

Here, you will attempt to ‘brainstorm’ the new capacities you want to build. Consider the following questions which may help you identify them:

- **Who/what** is under threat? What new capacities should the person or people under threat build in order to reduce the likelihood or impact of the threat identified?
- **Who** is behind the threat? How might you try to influence the cost-benefit analysis of the people or institution who might be behind the threat identified? Is there any way you can improve their tolerance or acceptance of our work, or deter them from acting against you?
- **How**: What information is necessary for them to carry out the attack? How can you further protect the sensitive information about your work and prevent it from falling into the wrong hands?
- **Where**: How can you increase the security capacities of the physical spaces around us (e.g. buildings, vehicles, private property) in order to make this threat less likely or damaging?

**Format &
Steps**

- **Psychological, emotional and health considerations:** In the context of this threat, what practices can you build to reduce stress and tiredness in order to be more aware and react more creatively to the threat?
-

3.2a

Exercise

Acceptance, deterrence and protection tactics

**Purpose &
Output**

In this exercise, you can further develop the new capacities you have identified as necessary to improve your security. Thinking about them in terms of acceptance, deterrence and protection strategies will help you get a sense of your overall security strategy and help you come up with additional tactics to develop.

**Input &
Materials**

If you want to write down the results of the exercise, consider using a format like the one in **Appendix D**.

**Format &
Steps**

- Step 1:** Look at the new capacities to build that you identified in **Exercise 3.1b**. Consider whether each of them is:
- an acceptance tactic
 - a deterrence tactic
 - a protection tactic
 - a combination of the above.
- Step 2:** Now, for each threat, consider further new tactics you could employ in order to:
- increase tolerance and acceptance of your work among your adversaries or society in general
 - dissuade your adversaries from taking action against you by raising the cost of an attack
 - protect yourself from threats and respond more effectively to them.

**Format &
Steps**

Continue to elaborate your list of new capacities with the new ideas you come up with.

Step 3: For each of the new capacities you have identified, consider the resources (financial and material) to which you will need access in order to build these capacities.

3.4

Exercise

Assessment of organisational security performance

**Purpose &
Output**

This is a basic exercise which checks perceptions of members of the organisation regarding the implementation of organisational security measures

**Input &
Materials**

Some drawing materials or a copy of the security wheel exercise (**Appendix E**)

**Format &
Steps**

You may want to focus on overall organisational security performance, or one more specific aspect of your organisation's security practices such as digital security, psycho-social well-being, travel security, security in conflict zones, etc.

Step 1: Take a copy of the organisational 'security wheel' (**Appendix B**) or draw a circle and divide it into eight Sections, each with a title (as in the diagram) to create your own security wheel.

Step 2: For each segment of the 'wheel', colour in a proportion which, in your opinion, reflects the extent to which your organisation implements best practices.

Step 3: For each segment, each person should identify the barriers which are currently preventing them or the organisation in general from better observing best practices

**Format &
Steps**

Step 4: Similarly, consider what the potential solutions are for each barrier or problem.

Step 5: Compare results among members of the organisations. Where is there consensus, and where are there differences? Why might that be?

Step 6: Together, try to identify areas which must be prioritised for improvement.
