6

Identifying and Analysing Threats

In this Chapter, we will build on our analysis to identify concrete threats to our well-being. Threats, for the purposes of this exercise, refer to any potential event which would cause harm to ourselves or our work.

The process of identifying and analysing threats is not new to us. In daily life, this is something many of us do naturally and almost without conscious effort. Crossing a busy street is fraught with possible dangers but those of us living in urban areas are usually able to do so safely, employing our ability to identify threats, such as an approaching bus or a motorist in a speeding car, and taking measures to minimise their ability to harm us.

In order to do this, we rely on our prior knowledge as well as processing new information. We take into account environmental factors (is the road surface wet due to rain?), social norms (crossing anywhere on the road in some cultures versus only using pedestrian crossings in others), and who possible allies and opponents are (a police officer, the driver of the bus). Some of our prior experience allows us to cross streets in unfamiliar places, but we may also need more information in a new situation, such as the norms and laws in another city. For example, cycling commuters and bicycle lanes in some European cities can be a surprising danger for someone who is used to interacting only with motor-vehicles when crossing streets. Similarly, in our work and activism, we are usually able to identify some of the threats we face and take steps to reduce or prevent them. However, with the context changing around us, we may encounter threats we do not notice or know about. Our preparations will help us have a more comprehensive picture of the threats we might be facing.

Through following the exercises in the previous Chapters, you may have accumulated a body of knowledge about your situation, including your vision, the environment in which you operate, your allies and opponents and their respective resources and limitations, what comprises your information assets and identifying security indicators which help you to remain aware of your security situation.

This information should leave us well prepared to identify threats to ourselves, our group or organisation. We can substantiate the threats we perceive by gauging the resources and abilities of our opponents, identify previously unnoticed threats to our information ecosystem and using the indicators in our preparations to prevent, defend against, respond to, or resolve such eventualities.

Note: It is, however, important to keep in mind that not all the threats to our well-being and security are political or related to our work. We should also be mindful of threats which may arise from delinquency, petty crime, gender-based violence, environmental hazards, etc. Although these do not necessarily represent a political response to our work, they can be among the most important threats to human rights defenders.

In this Chapter we can start with what we feel to be existing threats against us and scrutinise them. We will also use the previous steps in this Section as a starting point for identifying the underlying potential threats. Using the previous findings, we will then be in a position to evaluate these threats based on what we consider to be the **likelihood** that they would happen, and the extent of the **impact** or damage if or when they do.

Our response to them is also categorised similarly around the above two concepts and can be thought of as a combination of the **prevention** and **response tactics** we will employ. In the subsequent Chapters, we will come up with preparations and actions to minimise the likelihood of these threats, as well as steps and actions we will take to reduce the damage of threats that are carried out.

2.6a

Exercise

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

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 you work, should one of them occur.

Perceiving threats

As previously mentioned, our perception of threats is sometimes challenged for a number of reasons: perhaps the information available is limited; perhaps fear, stress or previous traumatic experiences have an impact on our perception and can lead us to experience unfounded fears ('paranoia') or to fail to recognise threats. Both of these occurrences are quite natural, although they are not desirable. Therefore, it's a good idea to be aware of this and find mechanisms for checking our perception – either through further research or through consultation with people we trust.

In the next exercise, we pose some questions which may help you to think critically about your perception of threats and devise tactics for making your perception more accurate.

2.6b Exercise

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.

Prioritising threats: analysing risk

As we begin the process of identifying all the threats or obstacles which may affect us or our work, it is important to avoid becoming overwhelmed. If we brainstorm threats, we may indeed come up with a long list and not know where to start; furthermore, this may be aggravated by unfounded or exaggerated fears. This is why, as in the previous steps, analysing each threat can be helpful. Threats can be viewed and categorised in light of the following:

- the likelihood that the threat will take place
- the impact if and when it does.

Likelihood and impact are concepts which help us determine risk: the higher the likelihood or impact of a threat, the higher the risk. If a threat is less likely or would have a lower impact, the risk is lower.

Of course, in undertaking such an exercise, we must be aware that we are relying on our own perception. As we explored in previous Chapters, our perception can face a number of challenges when we are tired or stressed, or when we talk about threats outside our area of expertise (for example, threats to digital information, for HRDs who are less comfortable with technology). It is important to keep this in mind, comparing our perceptions to the perceptions of others, and carrying out research where necessary to verify them.

Likelihood

To gauge the likelihood of the occurrence of a threat, we can make use several sources of information, including: the actor map we created, our analysis of historical security indicators, and our allies' experiences in similar situations. This process is not expected to deliver the exact probability of a threat actually occurring, but rather to help us prioritise those threats we deem imminent. Generally, they can be grouped into the following categories.

Unlikely to happen

These are threats for which there is little precedent and few favourable conditions to facilitate them. While we may choose to 'down-prioritise' these, we should keep them in mind, especially if their impact would be substantial (see below). Furthermore, it is important to record these, because as our socio-political context changes, their likelihood might also change.

Likely to happen

These are threats with clear precedents and/or very favourable conditions to facilitate them. These threats are prioritised for our next steps.

Unclear, or don't know

In some cases, our information and intuition may not arrive at the same answer, or there may not be enough information to comfortably categorise the potential threat into likely or unlikely. In this case, it is important to err on the side of caution:

- investigate further regarding the potential threat with the help of our allies and their experiences, trusted subject matter experts, or deliberations within our group, until we can safely put them into one of the above categories, **or**:
- move them to the 'likely' category anyway.

Impact

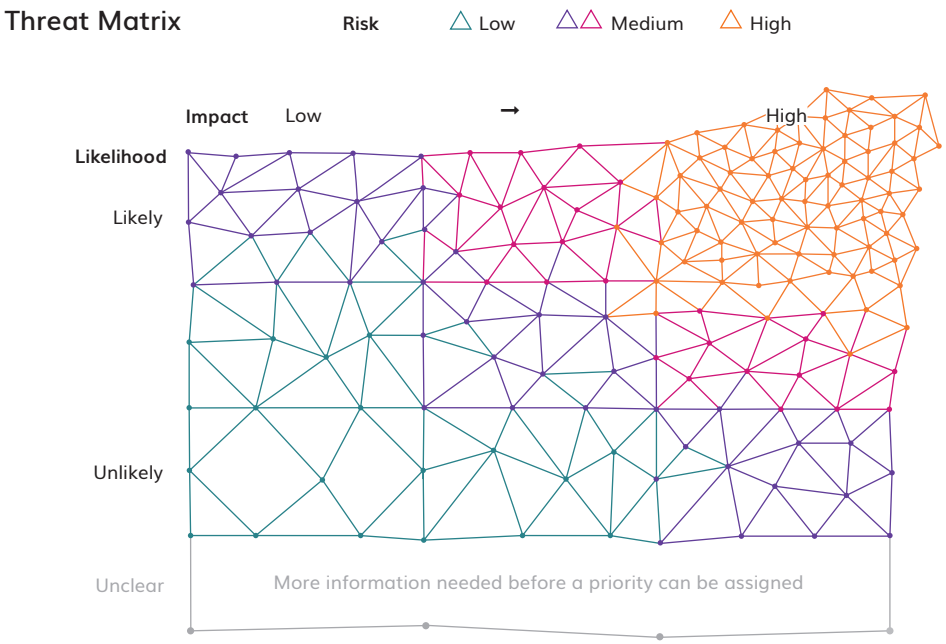
When analysing what the potential impact of a harmful event would be, it is helpful to imagine a scenario whereby the threat already took place. In this scenario, how has the threat harmed us? Examine the situation and reflect on questions like:

- How many people are affected?
- How long-lasting is the effect?
- To what extent does this hamper our normal operations?
- What other harmful situations does it enable?
- Is there an immediate danger to other people still not affected?

According to your own standards, you can consider the threats to be of low, medium, or high impact. Low-impact threats should only have limited negative impact on your ability to continue your work, whereas threats should generally be considered high impact if they would prevent you or your organisation from carrying out your activities effectively in the medium- or long-term.

It may help you to visualise the likelihood and impact of the threats you have identified by plotting them on a matrix such as in the example below, noting that

generally speaking, the priority threats – those which are 'higher risk' – will trend towards the upper right corner.



By considering the threats we identified in light of their likelihood and impact, we can then move towards a deeper analysis of them, the conditions required for them to happen and their potential consequences, which will aid us in planning to react to them.

Declared threats

Consider the possibility that we are faced with an explicit declaration of an intention to hurt us, e.g. a message from an individual, group or organisation that openly expresses their intent to cause us harm. These are also often referred to as 'declared threats' and are often made to human rights defenders in the form of text messages, phone calls, emails, verbal abuse or letters. They may alternatively be implied in our opponents' public statements or through judicial harassment, proposed legislation or many other methods. Their intention is to inflict damage on our work, to punish or hurt us and discourage others in turn. Such messages

constitute a special kind of security indicator because they already have an an impact (psychologically), and might well correspond to an actual threat. They deserve our attention to establish their veracity and severity.

Generally, 'declared threats' are:

Intentional they are made with a clear intent to intimidate us and discourage our work

Strategic they are part of a larger plan to prevent or hinder our work

Personal they are specific to us and our work

Fear-based they are meant to scare us so that we cease our work.[15]

It is important to keep in mind that while some threats may be real, others are intended to create new unfounded fears while no actual action to harm is planned by the individual or group who made the threat. When analysing this kind of indicator, you might find it helpful to go back to your actor-mapping and consider the resources and interests of the adversary in question.

Such threats are very 'economical', as they may achieve the same result as an attack, without the effort or possible expense of actually carrying it out. (As mentioned previously, identifying unfounded fears is an important part of developing an effective holistic security plan.) All the same, receiving such a message can itself be a very shocking experience and may inspire a lot of fear in us. It is important, as far as is possible, to create a safe space for ourselves or our group (emotionally, digitally and physically) in order to debrief, discuss, analyse and respond. For a suggestion of steps to take regarding analysing declared threats, see **Appendix C.**

Unfortunately, not all threats we may face are directly and explicitly noticeable. The results of our preparation in the previous Chapters are an invaluable resource for identifying, analysing and responding to threats we perceive. In this Chapter, we will employ our security indicators, our information ecosystem documents, as well as our actor and relational maps and situation analysis.

In the next exercise, we will begin with the list of threats we identified in the brainstorm, assign them a priority, and expand our understanding of their nature. It is important to also note that for many threats, our state of mind and body also plays a role in determining the probability as well as impact of any given threat.

---

15 See Front Line Defenders Workbook on Security for Human rights Defenders and Protection International: New Protection Manual for Human Rights Defenders http://protection-international.org/publication-page/manuals/

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).

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

Format & Steps

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 or 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?
- **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				

Now that you have identified a list of the threats that may arise in the course of your activities, along with who may be behind them, you can make plans and prepare for two inter-related objectives:

- to reduce the likelihood of the threat ever happening
- to minimise its impact if it does come to pass.

Remember that the above list is not a static list, and revisiting the process is very important. Shifts and changes in the context invariably affect the landscape of your work. Unforeseen threats may develop, or the likelihood of certain threats may be reduced due to external factors. You can determine how often you should revisit these lists and set time aside for it.

Conclusion

In **Section II | Explore**, we have followed a series of steps in order to analyse our context, beginning with the general (e.g. political, economic, social, technological, legal and environmental factors) and moving gradually towards identifying specific threats to our security.

In the next Section, we will take steps to prepare ourselves in order to reduce the likelihood of threats occurring and their impact, examining our existing capacities and vulnerabilities relative to these threats, and from there, building security strategies, plans and tactics.

We also have to consider how we can integrate these steps into our existing routines and work in order to maintain an up-to-date analysis of our context, and build consistent organisational approaches to managing our security and well-being.