

Understanding and assessing threats

Purpose:

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

Threats assessment: Understanding threats in depth

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

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

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

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

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

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

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

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

"Making" vs. "posing" a threat

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

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

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

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

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

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

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

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

The three main objectives when assessing a threat are:

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

Five steps to assessing a threat

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

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

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

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

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

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

For example:

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

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

Maintaining and closing a threat case

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

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

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

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

Reacting to threats in security terms

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

Summary

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

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

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

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

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

