

A ssessing risk: threats, vulnerabilities and capacities

Purpose:

Understanding the concepts of threats, vulnerability and capacity in security.

Learning how to do a risk assessment.

Risk analysis and protection needs

Human rights defenders' work can have a negative impact on specific actors' interests, and this can in turn put defenders at risk. It is therefore important to stress that **risk is an inherent part of defenders' lives in certain countries.**

The issue of risk can be broken down in the following way:

Analyse main stakeholders' interests and strategies → Assess impact of defenders' work on those interests and strategies → Assess threat against defenders → Assess vulnerabilities and capacities of defenders → Establish Risk.

In other words, the work you do as a defender may increase the risk you face.

- **What** you do can lead to threats
- **How, where, and when** you work raises issues about your vulnerabilities and capacities.

There is no widely accepted definition of risk, but we can say that risk refers to possible events, however uncertain, that result in harm.

In any given situation, everyone working on human rights may face a common level of danger, but not everyone is equally vulnerable to that general risk just by being in the same place. **Vulnerability** - the possibility that a defender or a group will suffer an attack or harm - varies according to several factors, as we will now see.

An example:

There may be a country where the Government poses a general threat against all kinds of human rights work. This means that all defenders could be at risk. But we also know that some defenders are more at risk than others; for instance, a large, well established NGO based in the capital will probably not be as vulnerable as a small, local NGO. We might say that this is common sense, but it can be interesting to analyse why this happens in order to better understand and address the security problems of defenders.

The level of risk facing a group of defenders increases in accordance with threats that have been received and their vulnerability and capacities to those threats, as presented in this equation¹:

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

Threats are the possibility that someone will harm somebody else’s physical or moral integrity or property through purposeful and often violent action². A threat assessment analyses the likelihood of a threat being put into action.

Defenders can face many different threats in a conflict scenario, including targeting, common crime and indirect threats.

The most common type of threat – targeting - aims to hinder or change a group's work, or to influence the behaviour of the people involved. Targeting is usually closely related to the work done by the defenders in question, as well as to the interests and needs of the people who are opposed to the defenders’ work.

Incidental threats arise at least from:

- being in **fighting areas in armed conflicts** ('being in the wrong place at the wrong time').
- **common criminal attacks**, especially if defenders’ work brings them to risky areas. Many cases of targeting are carried out under the cover of 'ordinary' criminal incidents.

Targeting (targeted threats) can also be seen in a complementary way: Human rights defenders may come across **direct (declared)** threats, for example by receiving a death threat (see Chapter 1.3, for how to assess declared threats). There

A summary of kinds of threats

- Targeting (direct/declared) threats, indirect threats): threats due to your work.
- Threats of common criminal attacks.
- Incidental threats: Threats due to fighting in armed conflicts.

¹ Adapted from *Van Brabant* (2000) and REDR.

² Dworken (1999)

are also cases of **indirect** threats, when a defender close to your work is threatened and there are reasons to believe that you might be threatened next.

Vulnerabilities

Vulnerability is the degree to which people are susceptible to loss, damage, suffering and death in the event of an attack. This varies for each defender or group, and changes with time. Vulnerability is always relative, because all people and groups are vulnerable to some extent. However, everyone has their own level and type of vulnerability, depending on their circumstances. Let's see some examples:

- ◆ Vulnerability can be about location: a defender is usually more vulnerable when s/he is out on during a field visit than when s/he is at a well known office where any attack is likely to be witnessed.
- ◆ Vulnerability can include lack of access to a phone, to safe ground transportation or to proper locks in the doors of a house. But vulnerability is also related to a lack of networks and shared responses among defenders.
- ◆ Vulnerability may also have to do with team work and fear: a defender that receives a threat may feel fear, and his/her work will be affected by fear. If s/he has no a proper way to deal with fear (somebody to talk to, a good team of colleagues, etc) chances are that s/he could makes mistakes or take poor decisions that may lead him/her to more security problems.

(There is a combined check-list of possible vulnerabilities and capacities at the end of this chapter.)

Capacities

Capacities are the strengths and resources a group or defender can access to achieve a reasonable degree of security. Examples of capacities could be training in security or legal issues, a group working together as a team, access to a phone and safe transportation, to good networks of defenders, to a proper strategy for dealing with fear, etc.

**In most cases,
vulnerabilities and
capacities are two sides of
the same coin.**

For example:

Not knowing enough about your work environment work is a vulnerability, while having this knowledge is a capacity. The same can be said about having or not access to safe transportation or to good networks of defenders.

However, in most cases
behaviour is a
determining factor

For example:

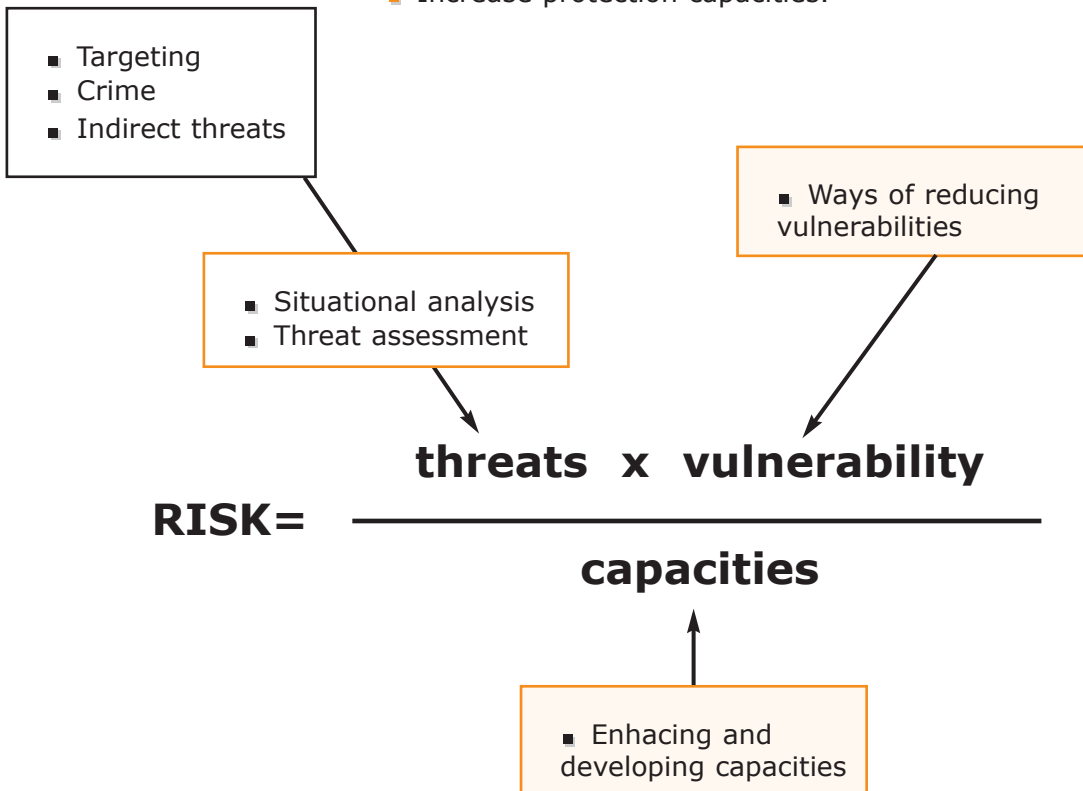
Having a phone can potentially be both a vulnerability and a capacity, depending on how it is going to be used. If it is used loudly and confidential information is communicated, it is a vulnerability. If it used discretely and confidential information is coded, it is a capacity.

(There is a combined check-list of possible vulnerabilities and capacities at the end of this chapter).

In summary,

in order to reduce risk to acceptable levels -namely, to protect- you must:

- Reduce threats.
- Reduce vulnerability factors.
- Increase protection capacities.



Risk is a dynamic concept that changes with time and with variations in the nature of threats, vulnerabilities and capacities. This means risk must be assessed periodically, especially if your working environment, threats or vulnerabilities change. For instance, vulnerabilities can increase if a change of leader-

ship leaves a group of defenders in a weaker position than before. Risk increases dramatically with a clear and present threat. In such cases, it is not safe to try to reduce risk by increasing capacities, because that takes time.

Security measures, such as legal training or protective barriers, can reduce risk by reducing vulnerability factors. However, such measures do not confront the main source of risk, i.e. the threats, nor the will to carry them out, especially in situations where perpetrators know they are likely to go unpunished. All major interventions in protection should therefore aim to reduce threats, in addition to reducing vulnerability and enhancing capacity.

An example:

A small group of defenders are working on land property issues in a town. When their work starts affecting the local landowner's interests they receive a clear death threat. If you apply the risk equation to their security situation, you'll see that the risk these defenders face is very high, above all due to the death threat. If you want to reduce that risk it is probably not the moment to start changing the locks on the door of their office (because the risk is not related to a break-in at the office), nor the moment to buy a cell phone for each defender (even if communication might be important to security it is unlikely to be enough if there is someone coming to kill you). In this case, a more relevant strategy would be to work on networking and generating political responses to directly confront the threat (and if that is unlikely to be effective quickly the only way to reduce the risk significantly might be to reduce the defenders exposure, perhaps by moving away for a while – being able to relocate to a safe place is also a capacity). Making and implementing such a decision also involves a psychosocial capacity for the defender to see that withdrawal is not a synonym of cowardice or defeat... Withdrawing can allow reflection and resuming work once better equipped.

Vulnerabilities and capacities, as well as some threats, may vary according to gender and age. You therefore need to break down your findings accordingly.

Vulnerabilities and capacities assessment

Designing a vulnerability and capacities assessment for a given group (or person) involves defining the group itself (a community, collective, NGO, individuals, etc), the physical area where it is located and the time line (your vulnerability profile will change and evolve over time). Then you can proceed to assess vulnerabilities and capacities, using the **chart 1.3** at the end of this chapter as guidance.

Please note: The vulnerabilities and capacities assessment must be seen as an open-ended activity aimed at building on existing information to maintain an accurate picture of a constantly evolving situation. When assessing vulnerabilities and capacities, it is important to first draw the current inventory and only then, list the potential and desirable ones. Later, you will need to establish a process to achieve the latter.

Chart 3: Information needed to assess a group’s vulnerabilities and capacities.

“Note: Generally speaking, the information in the right column shows vulnerabilities or capacities of each component”

VULNERABILITIES AND CAPACITIES	INFORMATION NEEDED TO ASSESS THE DEFENDERS’ VULNERABILITIES OR CAPACITIES IN RELATION TO THOSE COMPONENTS
COMPONENTS RELATED TO GEOGRAPHICAL, PHYSICAL AND TECHNICAL FEATURES	
EXPOSURE	The need to be in, or to pass through, dangerous areas to carry out normal daily or occasional activities, with threatening actors in those areas.
PHYSICAL STRUCTURES	The characteristics of housing (offices, homes, shelters); building materials, doors, windows, cupboards. Protective barriers. Night lights.
OFFICES AND PLACES OPEN TO PUBLIC	Are your offices open to visitors from the general public? Are there areas reserved only for personnel? Do you have to deal with unknown people that come to your place?
HIDING PLACES, ESCAPE ROUTES	Are there any hiding places? How accessible are they (physical distance) and to whom (for specific individuals or the whole group)? Can you leave the area for a while if necessary?
ACCESS TO THE AREA	How difficult is it for outside visitors (government officials, NGOs, etc.) to access the area, for example in a dangerous neighbourhood? How difficult is access for threatening actors?
TRANSPORT AND ACCOMMODATION	Do defenders have access to safe transportation (public or private)? Do these have particular advantages or disadvantages? Do defenders have access to safe accommodation when travelling?
COMMUNICATION	Are telecommunications systems in place (radio, telephone)? Do defenders have easy access to them? Do they work properly at all times? Can they be cut by threatening actors before an attack?
COMPONENTS RELATED TO CONFLICT	
LINKS TO CONFLICT PARTIES	Do defenders have links with conflict parties (relatives, from the same area, same interests) that could be unfairly used against the defenders?
DEFENDERS’ ACTIVITIES AFFECTING A CONFLICT PARTY	Do defenders’ work directly affect an actor’s interests? (For example, when protecting valuable natural resources, the right to land, or similar potential targets for powerful actors) Do you work on a specially sensitive issue for powerful actors? (such as land ownership, for example)

TRANSPORTATION OF ITEMS AND GOODS AND WRITTEN INFORMATION	Do defenders have items, goods or information that could be valuable to armed groups, and therefore increase the risk of targeting? (Petrol, humanitarian aid, batteries, human rights manuals, health manuals, etc.)
KNOWLEDGE ABOUT FIGHTING AND MINED AREAS	Do you have information about the fighting areas that could put you at risk? And about safe areas to help your security? Do you have reliable information about mined areas?
COMPONENTS RELATED TO THE LEGAL AND POLITICAL SYSTEM	
ACCESS TO AUTHORITIES AND TO A LEGAL SYSTEM TO CLAIM YOUR RIGHTS	Can defenders start legal processes to claim their rights? (Access to legal representation, physical presence at trials or meetings, etc.) Can defenders gain appropriate assistance from relevant authorities towards their work and protection needs?
ABILITY TO GET RESULTS FROM THE LEGAL SYSTEM AND FROM AUTHORITIES	Are defenders legally entitled to claim their rights? Or are they subjects to repressive internal laws? Can they gain enough clout to make authorities take note of their claims?
REGISTRATION, CAPACITY TO KEEP ACCOUNTS AND LEGAL STANDARDS	Are defenders denied legal registration or subjected to long delays? Is their organisation able to keep proper accounts and meet national legal standards? Do you use pirate computer software?
COMPONENTS RELATED TO THE MANAGEMENT OF INFORMATION	
SOURCES AND ACCURACY OF INFORMATION	Do defenders have reliable sources of information to base accusations on? Do defenders publicise information with the necessary accuracy and method?
KEEPING, SENDING AND RECEIVING INFORMATION	Can defenders keep information in a safe and reliable place? Could it get stolen? Can it be protected from viruses and hackers? Can you send and receive information safely? Can defenders differentiate top secret and confidential information? Do defenders keep information on them even during non-working time?
BEING WITNESSES OR HAVING KEY INFORMATION	Are defenders key witnesses to raise charges against a powerful actor? Do defenders have relevant and unique information for a given case or process?
HAVING COHERENT AND ACCEPTABLE EXPLANATION ABOUT YOUR WORK AND AIMS	Do the defenders have a clear, sustainable and coherent explanation of their work and objectives? Is this explanation acceptable, or at least tolerated, by most/all stakeholders (specially armed ones)? Are all members of the group able to provide this explanation when requested - for example at a checkpoint -?
COMPONENTS RELATED TO SOCIAL AND ORGANISATIONAL FEATURES	
EXISTENCE OF A GROUP STRUCTURE	Is the group structured or organised in any way? Does this structure provide an acceptable level of cohesiveness to the group?

ABILITY TO MAKE JOINT DECISIONS	Does the group's structure reflect particular interests or represent the whole group (extent of membership)? Are the main responsibilities carried out and decision-making done by only one or a few people? Are back-up systems in place for decision-making and responsibilities? To what degree is decision-making participatory? Does the group's structure allow for: a) joint decision making and implementation, b) discussing issues together, c) sporadic, ineffective meetings, d) none of the above?
SECURITY PLANS AND PROCEDURES	Are security rules and procedures in place? Is there a broad understanding and ownership of security procedures? Do people follow the security rules? (For more details, please see Chapter 1.8)
SECURITY MANAGEMENT OUTSIDE OF WORK (FAMILY AND FREE TIME)	How do defenders manage their time outside of work (family and free time)? Alcohol and drug use represent great vulnerabilities. Relationships can also result in vulnerabilities (as well as strengths) How are families and friends involved in the defenders' activities?
WORKING CONDITIONS	Are there proper work contracts for everyone? Is there access to emergency funds? Insurances?
RECRUITING PEOPLE	Do you have proper procedures for recruiting personnel or collaborators or members? Do you have a specific security approach for your occasional volunteers (such as students, for example) or visitors to your organization?
WORKING WITH PEOPLE OR WITH INTERFACE ORGANIZATIONS	Is your work done directly with people? Do you know these people well? Do you work with an organization as an interface for your work with people?
TAKING CARE OF WITNESS OR VICTIMS WE WORK WITH	Do we assess the risk of victims and witnesses, etc, when we are working on specific cases? Do we have specific security measures when we meet them or when they come to our office? If they receive threats, how do we react?
NEIGHBOURHOOD AND SOCIAL SURROUNDINGS	Are defenders well socially integrated in the local area? Do some social groups see defenders' work as good or harmful? Are defenders surrounded by potentially hostile people (neighbours as informers, for example)? Are supportive neighbours part of the defenders' alarm system?
MOBILIZATION CAPACITY	Are defenders able to mobilize people for public activities?

COMPONENTS RELATED TO PSYCHOSOCIAL IMPACT (GROUP/INDIVIDUALS)	
ABILITY TO MANAGE STRESS AND FEAR	Do key individuals, or the group as a whole, feel confident about their work? Do group/community members clearly express feelings of unity and joint purpose (in both words and action)? Are stress levels undermining good communications and interpersonal relationships? Do people have access to external psychological support and/or have developed internal psychosocial skills?
DEEP FEELINGS OF PESSIMISM OR PERSECUTION	Are feelings of depression and loss of hope being clearly expressed (in both words and action)?
COMPONENTS RELATED TO SOCIETY, CULTURE AND RELIGION	
DISCRIMINATION	Are defenders discriminated (both outside and inside the organisation) on the basis of gender, ethnicity, religion or different sexual orientation? Is there confusion between human, social, economic, identity, cultural and religious rights?
COMPONENTS RELATED WORK RESOURCES	
ABILITY TO UNDERSTAND WORK CONTEXT AND RISK	Do defenders have access to accurate information about their working environment, other stakeholders and their interests? Are defenders able to process that information and get an understanding of threats, vulnerabilities and capacities?
ABILITY TO DEFINE ACTION PLANS	Can defenders define and, in particular, implement action plans? Are there previous examples of this?
ABILITY TO OBTAIN ADVICE FROM WELL INFORMED SOURCES	Can the group obtain reliable advice? From the right sources? Can the group make independent choices about which sources to use?
PEOPLE AND AMOUNT OF WORK	Do the people or personnel available match the amount of work needed? Can you plan field visits in teams (at least two people)?
FINANCIAL RESOURCES	Do you have enough financial resources for your security? Can you manage cash in a safe way?
KNOWLEDGE ABOUT LANGUAGES AND AREAS	Do you know the languages needed for the work in this area? Do you know the area properly? (roads, villages, public phones, health centres, etc.)
COMPONENTS RELATED TO NATIONAL AND INTERNATIONAL CONTACTS AND MEDIA	
ACCESS TO NATIONAL AND INTERNATIONAL NETWORKS	Do defenders have national and international contacts? To visiting delegations, embassies, other governments, etc? To community leaders, religious leaders, other people of influence? Can you issue urgent actions via other groups? Do you have access to particular organisations or membership status that enhances your protection capacities?
ACCESS TO MEDIA AND ABILITY TO OBTAIN RESULTS FROM THEM	Do defenders have access to media (national, international)? To other media (independent media)? Do defenders know how to manage media relations properly?

A risk scales: Another way to understand risk

A scales provides another way to understand this concept of risk: This is something we might call ... a "risk-meter". If we put two boxes with our threats and vulnerabilities on one of the plates of the scales, and another box with our capacities on the other plate, we will see how our risk gets increased or reduced:

Fig. 1

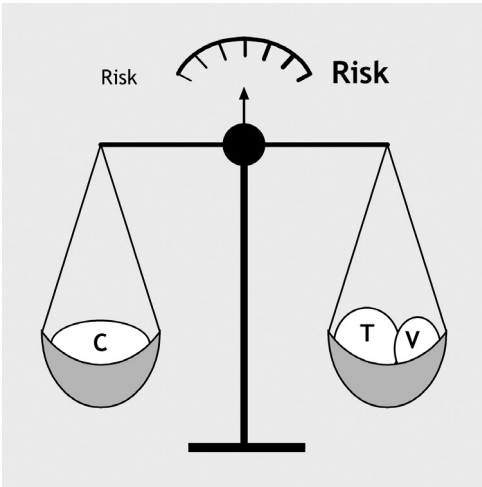
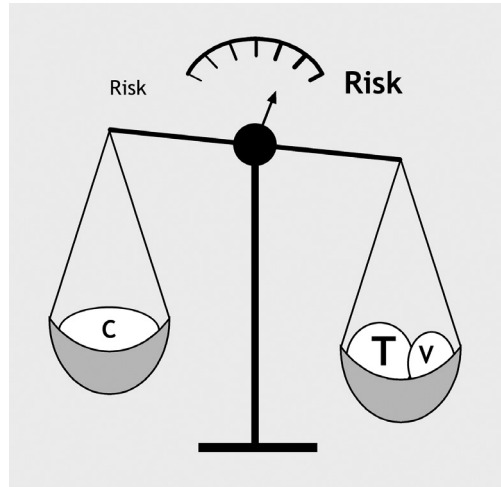
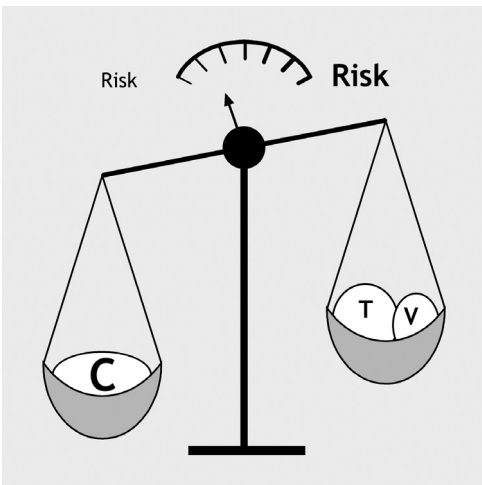


Fig. 2



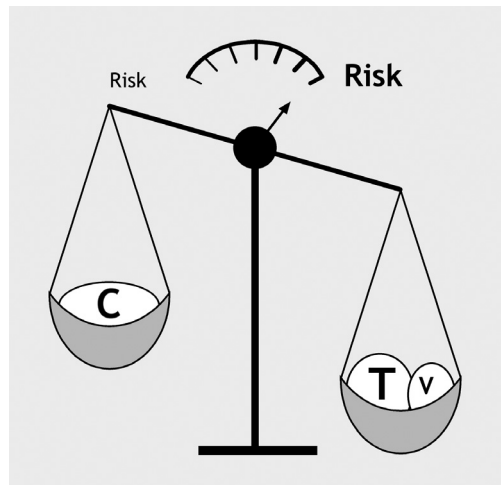
The more threats and vulnerabilities we have, the more risk we face.

Fig. 3



The more capacities we have, the less risk we face. And for reducing the risk, we can reduce our threats and our vulnerabilities, as well as increase our capacities.

Fig. 4



But ... Look at what happens if we have some big threats: Never mind we try to increase our capacities at that very moment: The scales will show a high level of risk anyway!

Summary

$$\text{RISK} = \frac{\text{threats} \times \text{vulnerability}}{\text{capacities}}$$

Vulnerability and capacities are internal variables (the defenders can work on them)

Threats are external variables (the threats can be made even if they are not feasible)

1 • Working on vulnerability and capacities will result in less feasibility of threats. List the current inventory of your vulnerabilities and capacities. Brainstorming can help.

2 • Separate them per global components and again, per specific components

3 • Set your desirable capacities: work towards them and consider the necessary process to achieve them.

Most of the time, a same set of actions can solve several items of a same component

4 • The result of the above steps will have as impact a reduced feasibility of the threat and therefore a reduced risk

Although some components may be linked to the environment, components can be considered as internal variables on which the defender can work: i.e. a dangerous area is, of course, "external" and yet, the defender can develop the skills ("internal") to deal with it.

A threat is external and whatever is done, the threatener might still threaten. The defender can "only" work on reducing the probability of the threat being put into action and not necessarily on eliminating the threat, unless the political context changes.

