

Building New Approaches to Security

Now that we have a clear idea of our current situation and some of the new capacities we need to build, we have already begun the process of building a new security strategy.

Having a strategy is different to having an ad-hoc or improvised approach to security. Many of our initial and instinctive reactions to threats, such as those we have identified already, may be effective at keeping us safe – however, some of them may not be, and may even be harmful. Therefore, as we begin to build new tactics, we should ensure that they relate to an overall strategy for **maintaining our 'space'** which in turn enables us to continue our work in the defence of human rights. Below, we will explore three archetypal strategies for maintaining our work space which we can draw on when designing our new approach to security.

Security strategies: Maintaining a space for our work¹⁶

When we consider developing one or more security strategies or plans, it's useful to remember that our strategies ought to correspond to the political, economic, social, technological, legal and environmental context in which we operate. There is no one-size-fits-all strategy.

In this respect, it can be useful to think of this in terms of the amount of space we enjoy for carrying out our work. The actors opposed to our work have the objective of shrinking that space, perhaps to the point where we can't carry out our work at all – hence the threats they impose upon us.

The point of a security strategy is to help us identify tactics and make plans in order to maintain or expand the space in society for our work, and this often involves engagement with the actors who oppose us, such as through advocacy or awareness-raising.

Some find it helpful to categorise these strategies as follows:

Acceptance strategies An acceptance strategy involves engaging with all actors – including allies, adversaries and neutral parties – in order to foster tolerance, acceptance and ultimately support of your human rights activities in society. Acceptance strategies might include running campaigns to build public support for your work or that of human rights defenders generally, or carrying out advocacy to develop positive relationships with local, State, or international authorities which correspond to their obligations to respect human rights defenders.

Protection strategies A protection or self-defence strategy emphasises learning new methods and implementing new practices or leveraging the strength of your allies to protect yourself and cover the gaps in your existing practices. Examples of practices which fall into this category might include implementing the use of email encryption or stress management practices within the group, or organising protective accompaniment or human rights observation during your activities.

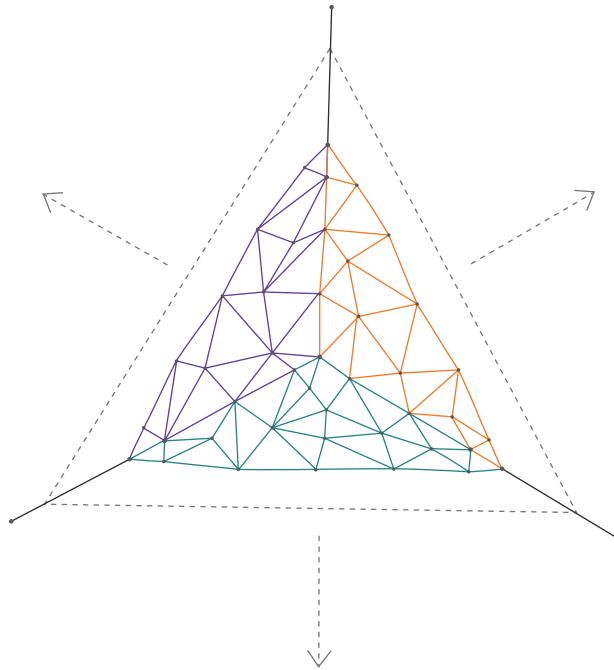
Deterrence strategies A deterrence strategy focuses on raising the cost of carrying out attacks against you or your work to your adversaries. If we return to the ‘spectrum of allies’ mentioned in [Section II | Explore](#), this strategy might include tactics to bring your active opponents into a position where their actions backfire on them in such a way that passive opponents or even other active opponents might (on moral grounds) shift to become neutral or even passive allies.¹⁷ Examples of other practices which fall into this category might include issuing an urgent appeal denouncing violations through a United Nations Special Rapporteur or taking legal action against an adversary who threatens you. These practices are most effective when you have a thorough knowledge of your adversaries and, ideally, are supported by powerful allies.

16 For more in-depth information on acceptance, deterrence and protection strategies, see Eguren, E. (2009). Protection International, New Protection Manual for Human Rights Defenders, Ch. 1.6

17 Martin, B. (2012) Backfire Manual: tactics against injustice. Irene Publishing, Sparsnäs, Sweden or Chenowith, E. & Stephan M.(2013) Why Civil Resistance Works. Columbia University Press.

Work Space

- △ Acceptance
- △ Protection
- △ Deterrence



Of course, these categories aren't mutually exclusive. Most human rights defenders will engage all three strategies in the course of their work, knowingly or otherwise, and some tactics could be seen as engaging two or even all three of the strategies simultaneously. However, this categorisation can still be useful as it helps us to think critically about the objectives of our security tactics.

In the case of organisations, it's particularly useful to recall these types of security strategies during the organisation's strategic planning process and to integrate security as a fundamental aspect of this.

Capacity building

Now that we have identified new capacities to employ in order to improve our security, we may have to undergo a process of capacity building which can take various forms: in our everyday life, we constantly engage in learning processes. In this case, we may simply need to identify and dedicate ourselves more explicitly to creating a new habit or making space in our work and personal life so as to develop new attitudes, knowledge and skills. Indeed, reading this resource is an example of this process. In [Section IV | Act](#), we can learn specific tools and tactics which are useful in particularly common scenarios for human rights defenders.

When we think about building new capacities, it can help to consider the five following factors which contribute to behaviour change:

- Well-being** If we want to learn anything new or undergo any process of change, we need to create the conditions in our body and mind to facilitate this process. This implies not only self-care in a physical and psychological sense but also means creating the necessary time and space in our daily schedules and consciously incorporating the learning processes into our routine, instead of seeing it as an additional burden to our existing workloads.
- Attitudes** are the extent to which we or those around us are open to the idea of changing our practices and see such changes as logical, necessary and valuable. Attitudes are subjective and can – like our perception of threat – be adversely affected by the experience of stress, fear and trauma. In [Section I Prepare](#) you can find more information about fostering positive attitudes in ourselves and our groups towards security.
- Knowledge** in this case refers to our understanding of the world around us, and in a practical sense, our knowledge of the political, economic, social, technological, legal and environmental context which impacts our security. In [Section II | Explore](#) you can find a series of steps which can be taken to improve our knowledge of our context from a security perspective.

Skills here refers to our practical ability to engage with and manipulate this environment, and can include everything from physical fitness and self-care, to political advocacy skills, technical skills like use of communication encryption, and so on.

Resources It's important to remember that we probably have a finite ability to improve our attitudes, knowledge and skills. The extent to which we can impact them is, among other things, a reflection of the resources to which we have access. This is often a challenge for human rights defenders, as well as people who are marginalised on the basis of their gender identity, religion, race, ethnicity, body type, social status, caste and so on, and is an important variable in our security planning.

In the next exercise, you can continue to elaborate on your existing capacities and the new capacities you brainstormed in **Exercise 3.1c**. You can categorise them according to whether they are acceptance, deterrence or protection tactics and get a sense of where there is space for you to further develop your capacities. Then you can consider the resources you have already or will need in order to build these capacities. Furthermore, in **Section IV | Act** online, you can find tips on concrete capacities to build for particular scenarios which may be of use.

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.

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.

External resources for capacity building

Once we have identified new capacities to build, it may become evident that we will need the help of external parties to facilitate this process. These may include consultants, experts, trainers on issues relating to well-being and security. Other required capacities may take the form of financial or material resources accessed through a funder or other intermediary organisation. Here, we explore some best practices and useful tips for engaging with these external resources.

External trainings and consultants

In some cases, it will be necessary to undergo a training or to involve an external security expert to explore the best ways of dealing with certain kinds of threats or emergencies.

External trainings and consultants are often very useful in helping organisations develop security plans and skills. Sometimes it is faster or more useful to call in external expertise, especially if none of your team members could attend a certain training or the context is very specific. On the other hand, preference might be given to getting training for your own colleagues or staff, as in this way external knowledge and skills are integrated into institutional knowledge.

Either way, in order to engage with consultants in a constructive and empowering way, it may be useful to think along the following lines. External consultants should:

- foster your empowerment and independence regarding your own security situation
- help you to have effective conversations about security
- understand security as personal and with a gender-justice perspective
- help you to conduct effective analyses of your own situation
- ask critical questions that you might not ask yourself
- train you on tools and tactics which you feel are relevant for your activities
- suggest possible solutions to problems based on experience in other contexts
- suggest other activists or organisations with whom you could exchange experiences
- suggest possible structures for policy documents and plans.

External consultants should not:

- conduct an analysis of your organisation's security practices for you (without involving members of the group)
- develop security plans for you
- provide security solutions for you
- provide security policies or plans for you
- make changes or take decisions for you
- claim to increase your security immediately... your own steps will increase your security!

Tips on how to choose adequate trainings or trainers

- Engage with experts who are trusted by friends or other human rights defenders.
- Be very clear about what you expect to learn but respect the opinion of the trainer in terms of what is achievable in the given time-frame.
- Clarify in advance whether you think the trainer is appropriate for you. Consider what kind of experiences or knowledge (for example, of your local context) they should have? What language is suitable for you? What time-frames? What location? How much time do you have afterwards for practising or working with the new skills, knowledge or resources?

Material resources for security

As the above exercise may have shown, building new security capacities can often have financial implications. Examples might include:

- replacing outdated hardware (such as computers) which may be vulnerable to attack
- hiring a part-time psychologist to support colleagues at risk of trauma
- working shorter hours and dedicating more time to analysing our security situation, which may have knock-on effects, e.g. for funding deadlines
- installing CCTV cameras at home or at the office to protect against break-ins.

While you may have existing resources which can be invested in such improvements, it is worth noting that there are a number of organisations who aim to make security improvements more affordable for human rights defenders. For a list of these, see the Holistic Security website.