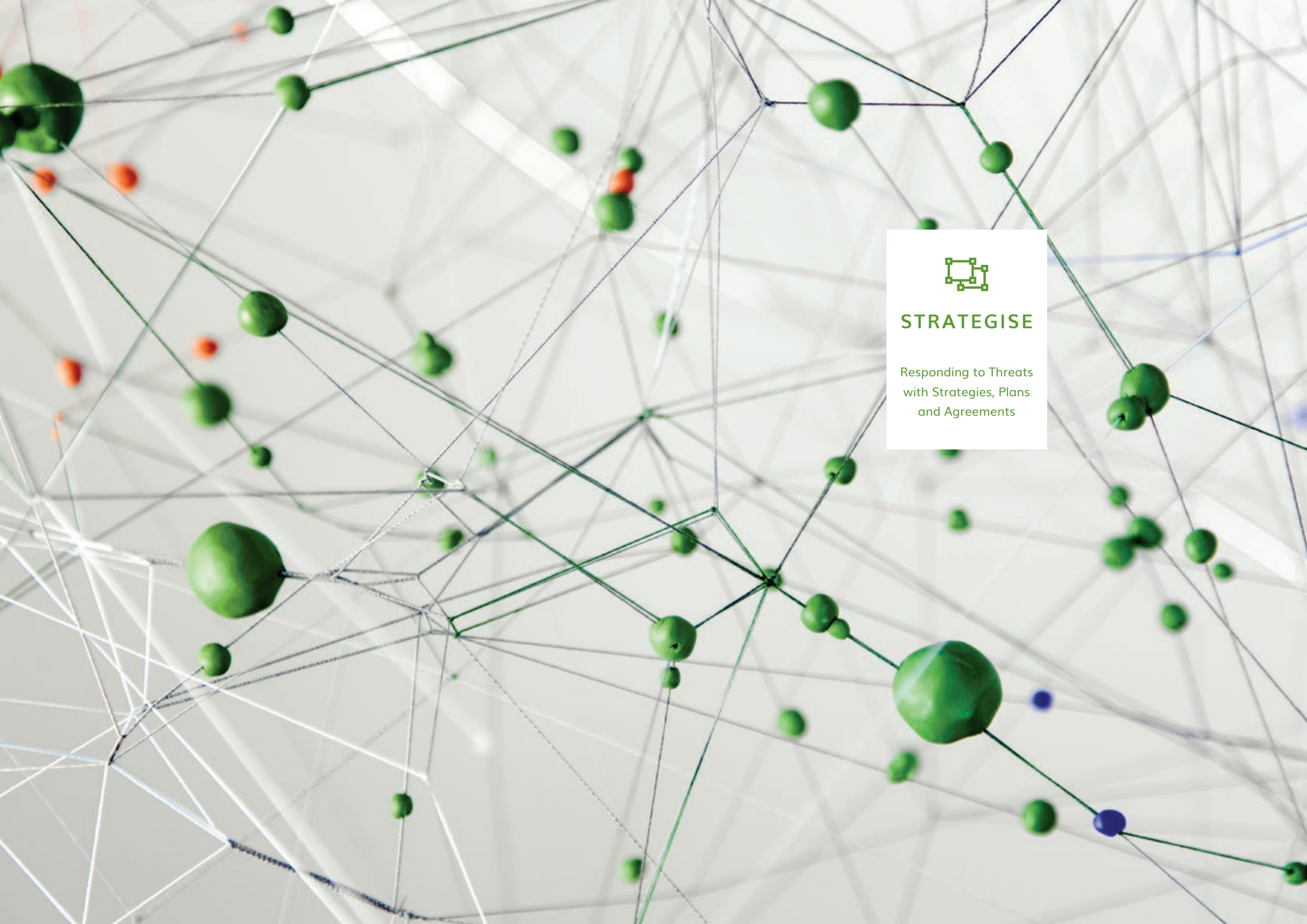


STRATEGISE

Responding to Threats with Strategies, Plans and Agreements

III Strategise

Responding to Threats with Strategies, Plans and Agreements

Contents

Introduction

In this Section, we will explore the process of developing and refining our security strategies, plans and tactics based on the threats identified in our context analysis. In order to do this, we must begin with the threats to ourselves, our work and our well-being that we identified in **Section II | Explore**. We will examine these threats in light of our current security practices, our capacities and vulnerabilities in order to establish the gaps that remain in our ability to properly respond to them.

Once we have completed a realistic assessment of our security situation, we can consider building new security strategies and formalising them into plans and agreements for different aspects of our work.

Alongside this process, we will consider some of the particular dynamics that arise for those of us who are trying to carry out security planning as an organisation, including assessments of organisational security practices, and engaging with the Do No Harm principle in security planning.

In Strategise, we will:

- examine our **capacities and vulnerabilities** relative to the threats we have identified
- identify **new** capacities we want to build and explore some key issues around security **capacity building**
- look at key elements for inclusion in **security plans** and the process of designing them
- explore key issues around security planning in larger **groups and organisations**
- engage with the **Do-No-Harm** principle and how it can be applied to our security practices.

1

Analysing our Responses to Threats

We will begin by analysing our existing security practices and responses to the threats we consider priorities. When it comes to security planning, very few of us will find ourselves starting 'from scratch': as mentioned before, we have certain instincts which help us to avoid or respond to threats in our daily life. Beyond that, we likely have certain socialised practices – often referred to as 'common sense' – which we unthinkingly practice in order to stay out of harm's way.

In this Section we are going to cast both an appreciative and critical eye upon these existing practices and identify steps we ought to take in order to develop security strategies, plans and tactics which correspond to the analysis we undertook in **Section II | Explore**.

Overall framework: Threats, capacities and vulnerabilities

In this process, it is useful to work with the concepts of capacities and vulnerabilities relative to each particular threat we identify.

- Capacities are the factors which help to keep us safer from a particular threat (i.e. reduce its likelihood or its impact).

- Vulnerabilities are the factors which make us more susceptible to a threat (i.e. they increase its likelihood or its impact).

Capacities and vulnerabilities may be characteristics of our own, our allies, or the environment in which we are operating which we consider relevant to our security.

Once we have identified our capacities and vulnerabilities as they relate to each threat we face, we can work on reducing our vulnerabilities and building our capacities in order to reduce the likelihood or impact of the threats: building capacities and reducing vulnerabilities help reduce the risk posed by a given threat.

Our existing practices and capacities

Using the threat analysis we carried out at the end of the last Section as a starting point, we will begin by analysing these threats in terms of our existing security practices and other capacities we can identify. Then, we can try to identify the gaps or vulnerabilities in our practices with a view to improving them.

We have already considered some of these existing practices for well-being and security generally in the previous Chapters but we'll now examine them in light of the threats we have identified. Even though this might be the first time that you have conducted a critical analysis of your security, some of your existing security and well-being practices may already be effective in preventing your high-priority threats from taking place. Security doesn't have to be complicated: it can include simple actions like locking the door to your office, having strong passwords for your online accounts or keeping a first-aid kit in your home.

However, it is important to avoid creating a false sense of security. We should think critically about our existing practices and whether or not they are truly effective in our context. The question is: how (if at all) do our existing practices relate to the threats we've identified?

In **Section II | Explore**, we considered our priority threats in great detail. We thought about:

- what the effects of each particular threat would be (if it came to pass)
- who may be responsible for the threat
- who or what would be the target of the threat
- how the threat would be carried out

- what information our adversaries would require for this
- where the potential attack would take place, and
- how our own mental and physical state may make us stronger, more resilient or conversely more susceptible and vulnerable to the threat.

In the next exercise, we will consider these questions in terms of our existing good practices.

3.1a

Exercise

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

Format & Steps

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?
- **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				

Identifying gaps and vulnerabilities

Now that we have identified our good practices and how they may relate to the threats we have prioritised, we should ask ourselves a slightly more difficult question: **What gaps remain** that may make us more vulnerable to these threats? What unhelpful attitudes or lack of sufficient knowledge or skills on our part represent vulnerabilities?

In navigating this question, it is important to remember that stress, tiredness and fear (among other factors) might inspire **unfounded fears**. Additionally, our resource limitations (or the sophistication of our adversary) may result either in inaccuracies when gauging the threats we recognise or in **unrecognised threats**.

Recognising such uncertainty where it exists is a positive first step which can propel us to **further investigate** the threats around us. We can also take steps to

check our perceptions by engaging in conversation as a group or with our trusted allies, colleagues and friends.

With that in mind, it is helpful to now return to your threat analysis and reflect on what details you know about the threats you face and your existing practices for preventing or reacting to them. Where are the gaps and vulnerabilities in relation to each of the aspects you considered?

3.1b Exercise

Vulnerabilities and gaps in our existing practices

Purpose & Output

In this exercise, you can consider each of the threats you identified and prioritised in **Section II | 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?
- **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				

Identifying the gaps in our security practices can be unnerving but it's an important step in developing the wisdom which will help us to build better security plans. Once we have identified these gaps, we can consider what resources and knowledge we need to build and develop plans and agreements with clear objectives with regard to security.

Identifying new capacities

By now, we should have a good idea of the threats we face, our capacities relative to each of them (including our existing practices) and our vulnerabilities relative to each of them, which should also highlight where there are gaps and room for improvement in our practices. Basing ourselves in this analysis, we can now identify **new capacities to build** in order to improve our well-being in action.

It is useful, therefore, to carry out an initial brainstorm of these new capacities. In the following Chapters, we will explore some of the dynamics around how to develop and implement them.

3.1c Exercise

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 in a format such as 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?

Format & Steps

- **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?
- **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?

At this point, it may be a good idea to collate your notes from all the previous exercises to get a clear idea of your current security situation and some of the new capacities you require to deal with the threats you face.

In the next Chapters, we will consider some of the dynamics around building these new capacities and developing them into an overall security strategy and set of security plans.

2

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 work[16]

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

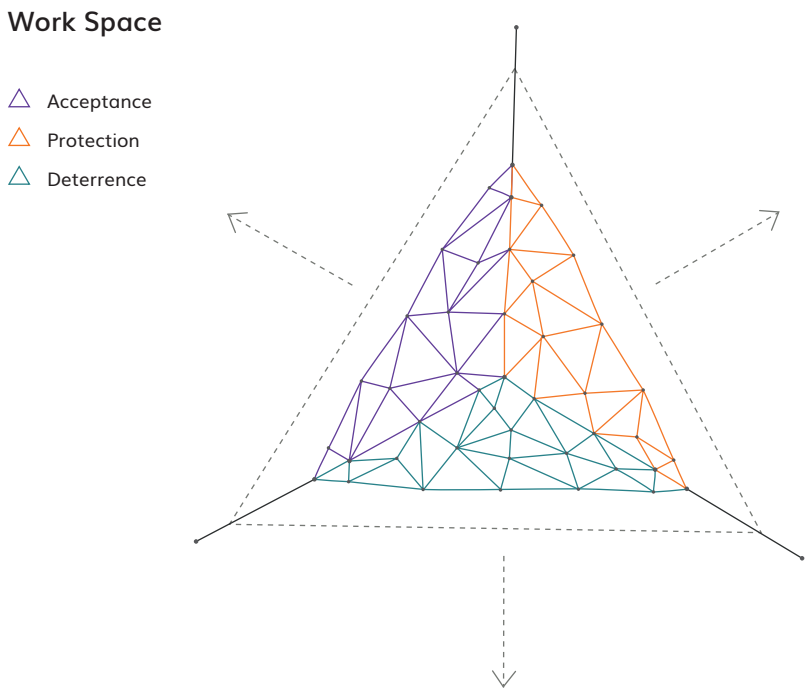
A protection or self-defence strategy emphasises learning new methods and implementing new practices or leveraging the strength of your allies to protect yourself and cover the gaps in your existing practices. Examples of practices which fall into this category might include implementing the use of email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

---

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

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.



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.

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.

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.

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.

3

Creating Security Plans and Agreements

The logical conclusion of the process we have followed thus far – diagnosing our security situation, our capacities and vulnerabilities and identifying new capacities to be built – is to create or update our plans or agreements relating to security as we go about our human rights work. These plans can be formal, written documents or informal, shared agreements, depending on the culture of your group or organisation. The most important thing to remember is that they are **live agreements or documents** and should be subjected to regular updates by repeating the steps we have taken up to this point.

We can organise these plans and agreements according to a logic which suits us, such as:

- by activity (e.g. a protest plan, or a plan for monitoring and documentation missions)
- by region (e.g. a plan for operating in conflict zones, a plan for work in rural areas)
- by individual (e.g. a plan for lawyers, a plan for the finance department)
- by day of the week according to a set working pattern
- by any other metric which corresponds to our work.

Creating security plans and agreements may not necessarily be a new activity for us. In fact, in everyday life, we make and implement security plans all the time. For example, every time you leave your home for a long period of time, you might reasonably decide to lock the doors and ensure that all the windows are closed, and perhaps even have a friend or neighbour keep an eye on it. Although it may seem like simple, common sense, this qualifies as a security plan.

What differentiates human rights defenders from other people is that our work requires us to take a more organised approach to security planning. We may need to have more security plans than usual and suffer from higher levels of stress than others. Therefore, it's a good idea for us to be organised and explicit – within our organisation, our group or just with ourselves – about how we behave in certain circumstances.

Elements of security plans and agreements

There are a number of ways we can organise our security plans or agreements, according to the way we work or whatever feels most practical. However, most good security plans will serve one or both of the following purposes:

Prevention of threats Most security plans will include tactics which aim to prevent identified threats from taking place (i.e. reducing their likelihood). Examples of prevention tactics might include encrypting a database of contacts so as to reduce the likelihood that it can be accessed by adversaries, or employing a security guard at the office so as to reduce the likelihood that it is broken into.

Emergency response Also called contingency plans, these are the actions which we take in response to a threat becoming a reality. They generally have the aim of lessening the impact of the event and reducing the likelihood of further harm in its aftermath. Examples of emergency response tactics might include bringing a First Aid kit with you when travelling, in case of minor injuries, or a mask and goggles to a protest in case tear gas is used.

Both purposes are explained in more detail below.

Prevention of threats

As mentioned, preventative measures involve employing tactics that help us to **avoid** a threat or reduce its likelihood.

Many of these tactics will reflect strategies of **acceptance, deterrence** and **protection or self-defence**, as explored in the previous Chapter. As such, they may include advocacy campaigns or other forms of engagement with the public or civilian and military authorities in order to raise consciousness and acceptance of the legitimacy of our work; strengthening of ties with our allies in order to raise the potential cost of aggressions against us, and any number of tactics which build our own capacities and agility in the face of the threats to our work which we have identified.

Although these kinds of measures which may at first require time and space to implement, they soon become a 'normal' aspect of our work and personal lives.

Emergency plans

Unfortunately it's a fact of life that even the best laid plans may fail us, especially in the case of security incidents. These are the moments where, perhaps due to rapidly changing circumstances, we experience an aggression or accident which we thought we could prevent.

In these cases, it's imperative to have plans in place to reduce the impact on us, and our friends, family, or organisation.

As discussed, there are some common occurrences which everyone should plan for and which may have nothing to do with our human rights activities. For example, we might have a first-aid kit at home, just in case an accident should happen in the course of our day – even while we're just cooking or cleaning! Although it may seem like common sense, this is a realistic and (hopefully) effective contingency plan: in the case of a minor household accident, a well-stocked first-aid kit will help you recover more quickly.

As human rights defenders, we also have to prepare for common incidents which may arise from our geographical, social, economic or technological contexts such as:

- natural disasters, accidents
- theft or violent crime, unrelated to our work
- data loss
- events of emotional significance, such as problems in our family or personal relationships, which may also affect our security.

Additionally, as we have learned through the exercises up to this point, there are also threats which are directly related to our work and the activities we undertake therein. Common examples during an activity such as protesting might include:

- arrest
- physical harassment or
- being affected by tear gas.

Our prevention tactics and emergency plans usually deal with the same threats; first seeking to reduce their likelihood, then attempting to lessen their impact after they occur. As such, these tactics are 'two sides of the same coin', and most good security plans will include both. While in a prevention plan, we define our actions to reduce the likelihood of harm, in an emergency, our aim is to reduce the harm that may be sustained, prevent others from being affected, and to deter the aggressor (where there is one) from carrying out further harm.

Well-being and devices

Some important aspects commonly forgotten in security planning are tactics for our well-being and tactics for managing our devices and information. Well-being in this case refers to actions we take to maintain our physical energy and a mindful approach to our work and our security – it may include such considerations as where and when we will eat, sleep, relax and enjoy ourselves in the course of our work. Devices and information refer to which devices we will depend on in order to carry out our work, and the tactics we will employ in order to ensure that our information and communication can not be accessed by others.

As far as individual human rights defenders are concerned, a simple security plan may look something like this:

Objective

Mission to collect testimonies of victims of human rights abuses in a rural area.

Threats

- Harassment or arrest by police.
- Confiscation of computer, mobile phone.
- Loss of data as a result.
- Compromising victims' anonymity as a result.

Prevention - actions and resources

- Alert colleagues and friendly embassies and international organisations of the mission, its duration and location.
- Share contact details of local authorities/aggressors with embassies and international organisations.
- Check-in with colleagues every 12 hours.
- Testimonies will be saved to encrypted volume immediately after writing.
- Testimonies will be sent encrypted with GPG to colleagues every evening.
- Email inbox and sent folder will be cleaned from the device after use.
- Security indicators and check-ins will be shared over an encrypted messenger.

Response - actions and resources

- Prepare an alert message (code) to send in case of surveillance/ being followed.
- Prepare an alert message (code) to send in case of arrest.
- Have lawyer's number on speed-dial.

Emergency plan

- In case of arrest, send alert message and call lawyer.
- On receiving alert message, colleagues will alert friendly embassies and international organisations.
- Ask for urgent appeals to be sent by international organisations to authorities.
- Hand over password for encrypted volume if under threat of abuse.

Well-being considera-tions

- Eating in a decent local restaurant, at least twice a day.
- Switching off mobile phone and all other devices during meal-times.
- Calling family over a secure channel to connect every evening.

Devices and information

- Mobile phone with encrypted messenger and call apps.
- Computer with encrypted volume and encrypting emails with GPG.

However, the example above still implies the cooperation of allies in order to build strategies of acceptance and deterrence. When it comes to groups or organisations, the process of planning may involve a few extra steps to ensure all voices are heard in the process, which is explored in the next Section.

Furthermore, as mentioned in **Section I | Prepare**, having solid, up-to-date security plans are a great accompaniment for our **resilience and agility** – but not a replacement for them. While it is a great help to undertake a process of analysis and planning which is as rational and objective as possible, as we know, we must also be prepared for the 'unexpected'. In this regard, we must also develop a sense of centredness and calm which will be of use to us when situations arise for which we have not – or could not have – made a plan. Security plans and agreements are therefore important and useful tools, as is the ability to be agile and let them go if the situation requires it.

4

Security in Groups and Organisations

There are a number of additional issues which arise when we approach security planning from within a structured group or organisation. Organisations develop their own hierarchies, cultures, strategies and means of planning into which the process of building security strategies and plans must 'fit'.

The process of planning for security in a group can be stressful for a number of reasons. It forces us to accept the genuine possibility of unpleasant things happening to us in the course of our work which can cause us or our friends and colleagues to become emotional or scared. It can also be difficult to consider all the possible variables and come to practical agreements about them.

Furthermore, in order to achieve organisational change successfully, we have to identify a process which can be both sufficiently inclusive and respectful of existing hierarchies where necessary. We must also recognise the personal nature of security and the need for the change to be managed in a way which encourages openness and recognises the distinct needs of different members of the group in accordance with not only the threats they face, but also aspects such as gender identity.

In this Chapter, we explore some of the key issues around building and improving security strategies and plans within organisations.

Creating and maintaining security plans

It's important to keep the following in mind when creating security plans following a risk analysis as explored in the previous segments, as part of a group or organisation.

Achieving buy-in

When introducing new people to existing plans in particular, it's important to go through some key points of the previous steps so that they understand how you arrived at the conclusion that these threats are plausible enough to plan for. Remember, as we explored in **Section I | Prepare**, security can be a very difficult issue to tackle as it is wrapped up not only in our physiological instincts, but also in our individual experiences of stress, tiredness and trauma. We

must remember to be patient and compassionate and work with our friends' and colleagues' perceptions rather than anything we consider (perhaps falsely) to be 'objective'. It's important not to scare people, but rather to try to create a relaxed and safe space in which people can express their questions and concerns and make commitments to act in a certain way during emergencies.

Participatory design

Some people will not react particularly well to having a security plan or agreement set without their consultation. High-risk activities and emergencies can be very distressing situations and it's important that each person is comfortable with the role and responsibilities they are assigned and has a space to express their concerns about this. In this regard, it's important that the process of security planning be as open and participatory as possible while still requiring a minimum commitment from all of those involved.

Role-playing

In some cases, it may be useful to design a role-play so that members of the organisation can practice how to respond to a certain emergency. Of course, this should be done carefully: avoid carrying out role-plays which may cause any team members to become distressed, especially those who have been victims of violations in the past. Be sure to get a sense of how organisation members feel about any role-play idea in advance and give them the opportunity to opt out if necessary.

Re-planning and considerations

Remember that all security plans should be live documents and processes. Once 'written' or agreed upon, they should not just be put in a drawer or on shared drive never to be read again! Rather, they should be re-evaluated and discussed regularly, especially when new members join the group in order to facilitate their acceptance and to allow new members to become familiar with them. Make it part of your security planning to include fixed dates to review your security practices and plans. It is also useful to include security issues in your strategic planning process to make sure security is not an afterthought. Doing this helps to ensure that security considerations are part of how you devise your strategy, develop activities, make necessary budget allocations and pro-actively address existing capacity gaps.

Emergency planning in groups and organisations

Like individual human rights defenders, groups and organisations ought to make emergency or contingency plans too in case our attempts to reduce the likelihood of an aggression or accident fail. When creating such plans in a group or organisation, here are a few key elements to keep in mind.

Definition of emergency

The first step in creating an emergency plan is to decide at what point we define a situation as an 'emergency' – i.e. the point at which we should begin to implement the actions and contingency measures we planned. Sometimes, this will be self-evident: for example, an emergency plan for the arrest of a friend or colleague would probably define the moment of arrest as the point at which an emergency should be declared. In other cases however, it may be less obvious: if a colleague carrying out a field mission stops answering their phone and can't be reached by other channels, how long should we wait before defining the situation as an emergency? These are agreements which, in the case of each threat, will have to be decided by you, your friends and your colleagues.

Roles and responsibilities

Depending on the number of people involved (be they your affinity group, collective, organisation, etc.), it is helpful if each person has clear roles that they are aware of and have agreed to in advance. This should help reduce disorganisation and panic in the event of an incident. In the case of each threat, consider the roles that you may have to assume and the practicalities involved in responding to an emergency.

In many cases, an important strategy for emergencies is the **activation of a support network**. A support network consists of a broad network of our allies, which may include our friends and family, community, local allies (e.g. other human rights organisations), friendly elements of the State, and national or international allies such as NGOs and allied journalists. Activating a support network, or some elements of it, during an emergency can greatly raise the cost of the aggression for those responsible and cause them to cease further attacks.

Return to your actor map (established in **Exercise 2.3 a/b**) and consider, for each threat scenario, the ways in which your allies may be able to support you. It may be useful to establish contact with them and verify that they will be willing to help you and know what you expect them to do in cases of emergency. In the case of State officials, it is good to consider this in terms of their position and perhaps

make reference to any local or international laws that would be useful in justifying this.

Channels of communication

Coordinating a response to an emergency always involves coordination of actions and often a lot of improvisation. In this regard, digital communication is increasingly important. It's important to establish what the most effective means of communicating with each actor is in different scenarios – and to identify a secondary means for back up too. Be aware that for emergencies, it might be useful to have clear guidelines on:

- what to communicate
- which channels to use (consider the sensitivity of the information, and the security of the channel: is it encrypted?)
- to whom?

Early alert and response system

An Early Alert and Response System is a useful tool for coordinating our response to an emergency – which may begin in the event of an accident or attack, or when there are very strong indicators that one is imminent. The Early Alert and Response System is essentially a centralised document (electronic or otherwise) which is opened in response to an emergency and includes:

- all the details about the security indicators and incidents which have occurred, with a clear time-line
- clear indicators to be achieved which will signify that the risk has once again decreased
- after-care actions which must be taken in order to protect those involved from further harm and help them to recover physically and emotionally. In some cases, it will be important to consult professionals to establish the best conduct – for example in case of traumatic events, physical or sexual violence, or accidents involving dangerous materials
- a clear description of actions which have been taken and will be taken in order to achieve these indicators, with a time-line.

The Early Alert and Response System provides useful documentation for subsequent analysis of what has happened and on how to improve our prevention tactics and responses to threats in the future.

Improving organisational security management

Beyond the creation of a strategy or series of individual security plans, organisations have to consider security management and its implementation by managers, staff and volunteers as a process of consistent re-evaluation. Organisations which implement the correct security measures perfectly at all times are rare and there will probably always be room for improvement. Bearing this in mind, it's a good idea to regularly evaluate the extent to which our security strategy and plans are not only consistent with the context in which we're operating (see **Section II | Explore**), but also that they are accepted and implemented by members of the organisation.

Assessment

While we'll often be aware that there is room for improvement in our implementation of security practices, it can sometimes be overwhelming to identify where to start, what to prioritise and who should be involved. It's useful to carry out an assessment of the current situation which will help us to identify in more detail the particular aspects of organisational security management which we need to improve.

This assessment and subsequent process of improvement will need to be managed, coordinated and carried out by people either internal or external to the organisation. Internal staff who could be involved may include:

- the board of directors and executive directors
- management or senior staff
- regular staff and volunteers.

External entities who could be involved in the process would include:

- donors
- external consultants and trainers.

Involving each of these actors in the process has its own distinct advantages and disadvantages.[18] However, bearing in mind the personal nature of security, it is important that from the outset, the process is carried out in an inclusive,

18 For more detail on this see Chapter 1.3 "Managing organisational shift towards an improved security policy" in the New Protection Manual for Human Rights Defenders (2009) Protection International.

participative, transparent and non-judgemental manner. Formal hierarchies within organisations can often become a 'sticking point' when it comes to managing a sensitive and personal process such as this; it is important that management remains sensitive and aware of the needs of their programme and 'field' staff or volunteers, who are often those putting themselves at higher risk and/or benefiting less financially from their activism. Staff and volunteers should also respect the fact that management face a difficult task of standardising an approach to security and are doing so, hopefully, in the best interests of all.

Criteria for assessment

As mentioned, a logical first step in improving organisational attitudes, knowledge and skills regarding security is to carry out an audit of the current situation in order to identify the priorities for improvement.

In assessing how the organisation's security protocols are observed and implemented by management, staff and volunteers, it is important to look at some concrete issues and indicators, in order to avoid becoming overwhelmed. It may be useful to consider the following points:[19]

Acquired security experience

How much experience of implementing security practices exists among members of the organisation? Is this experience spread evenly across staff, or concentrated among a few individuals?

Attitudes and awareness

Are people aware of the importance of security and protection? Is their attitude towards it generally positive? Are they willing to continue improving? What are the barriers they perceive to this? Consider whether this fluctuates between attitudes and awareness regarding digital security, physical security and psycho-social well-being.

Skills, knowledge and training

As previously mentioned, in order to build new knowledge and skills, resources, time and space need to be made available for training (either formal or informal). Is such training available to members of the organisation? Does this include trainings on psycho-social well-being and digital security?

19 Based on Chapter 2.1 "Assessing organisational security performance: the security wheel" in the New Protection Manual for Human Rights Defenders (2009) Protection international.

Security planning

To what extent is security planning integrated into our work? How often are context analyses (see **Section I | Prepare**) carried out and security plans created? Are plans updated regularly, and do they include digital device management and stress management?

Assignment of responsibilities

Is there a clear division of responsibilities for implementation of our security practices? To what extent are these responsibilities observed, and what are the potential blockages?

Ownership and compliance

To what extent are organisation members involved in the organisational security planning, and to what extent do they observe the plans that exist? What are the problems which arise here, and how can they be overcome? How can the process be made more participative?

Response to indicators

How often are security indicators shared and how often are they analysed and subsequently acted upon if necessary

Regular evaluation

How often are the security strategies and plans updated? Is there a concrete process in place for this, or is it ad hoc? How can it be made more regular, what other problems exist and how can they be overcome? In the exercise below, you can explore some concrete questions to help establish the extent to which security plans are observed within your organisation.

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: Use the organisational 'security wheel' (**Appendix E**) 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

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.

Prioritising areas for improvement

Once an assessment of the current situation has been carried out, we should have an idea as to which areas should be prioritised for improvement. A plan for improvement should be drawn up on this basis, and disseminated among the staff and management. The plan should:

- have a clear objective in terms of new best practices to be implemented
- a time-line, including who needs to be involved in the process and what is expected of them
- clearly stipulate the resources needed for the improvement to be made.

Management should ensure that staff and volunteers are granted the time to undergo any required training or other capacity building necessary in order for this improvement to take place.

Overcoming resistance to security planning[20]

It is often the case that, within organisations, there is resistance among some management, staff, or volunteers to the security protocols they are expected to observe. There can be a large number of reasons for this.

When attempting to deal with resistance to security planning within the organisation, it's important to keep in mind that, as we have explored previously, security is a deeply personal concept. As such, people may have particularly personal reasons for resisting certain protocols which imply changes in their personal lives, their free time, or their relationships; they may also imply having to learn new skills which are challenging and taxing on their energies which may already be under stress.

The best approach to dealing with resistance to changes in security practices, therefore, is to create a safe space in which individuals can comfortably voice their concerns around it. As noted in **Section I | Prepare**, it is a good idea to practice active listening and non-violent communication in order to facilitate an open and constructive debate.

Below are some common resistance stereotypes, the reasoning underlying the resistance and possible responses to help defenders overcome resistance within their groups, organisations, or communities. Seeking to create space for discuss-

20 Based on material from Chapter 2.3, New Protection Manual for Human Rights Defenders (2009) Protection International, p.153.

ing security within a group where everyone's opinion and experience is respected and heard is key. Being aware of personalities, power dynamics and hierarchies is important when deciding on responses to overcome resistance.

Common Resistance Stereotypes

"We're not being threatened" or
"Our work is not as exposed or contentious as other organisations' work."

Reasoning behind the stereotype

The risk stays the same, it doesn't change or depend on the fact that the work context might deteriorate or that the scenario might change.

Responses to overcome resistance

Risk depends on the politicalcontext. As the political context is dynamic, so is the risk.

"The risk is inherent in our work as defenders" and
"We are already aware of what we are exposed to."

Reasoning behind the stereotype

The defenders accept the risk and it does not affect them in their work. Or, therisk cannot be reduced, the risk is there and that's all there is to it.

Responses to overcome resistance

- Meeting with inherent risk does not mean accepting the risk.
- The risk has at least a psychological impact on our work: at the very least it induces stress which affects the work and possibly the personal well-being of the defender and the group.
- Risks faced by defenders are made up of various elements – threats as the external force seeking to impede or stop their work, defenders' vulnerabilities and capacities in relation to the threat(s): vulnerabilities and capacities as variables that a defender can influence. By identifying and analysing threats and their risk, defenders are able to realise existing vulnerabilities and capacities/strengths and undertake targeted efforts to reduce their vulnerabilities and increasing capacities. This will reduce the risk even if it is not entirely eliminated. Creating space in an organisation to analyse risks and jointly agree on strategies to reduce them can have an empowering effect on individuals and the group, increasing the individual and collective sense of security to continue their work.

"We already know how to handle the risk", or
"We know how to look after ourselves" and "We have a lot of experience."

Reasoning behind the stereotype

The current security management cannot be improved and it is therefore not worth doing. The fact that we have not suffered harm in the past guarantees that we won't in the future.

Responses to overcome resistance

- Security management is based on the understanding that risks faced by human rights defenders result from the political environment and the impact their work has on different actors' interests. Because this context is dynamic, risk is also dynamic, requiring constant analysis and adaptation of strategies. In addition, stakeholders change their position and strategies, also necessitating adaptation by human rights defenders to manage risks.
- Experience in advancing human rights and defending the rights of others requires you to constantly evaluate your strategy, create space for your work, identify support. This is the same when managing your security. If you want to have an impact with your work and protect the people you work for and with, you need to stay well and safe. And at the same time there is a somewhat moral obligation for you to not put the people you work with at further risk.

"Yes, the issue is interesting, but there are other priorities."

Reasoning behind the stereotype

There are more important issues than security of defenders.

Responses to overcome resistance

- First and foremost, defenders are people. They have families, friends, communities who need them and whom they need. Self care is a political act. Defenders' adversaries aim to cause harm, fear, anxiety and/or stress to hinder or stop their work. Being alive and well is a prerequisite to continuing a struggle against injustices.

"And how are we going to pay for it?"

Reasoning behind the stereotype

Security is expensive and cannot be included in fundraising proposals.

Responses to overcome resistance

- Thinking of one's security is not a weakness, it is a strength that will ultimately benefit the people you work with and for.
- Security is a very individual concept. In many cases it is closely related to defenders' attitudes and behaviours. Improving one's security often requires a change in attitude and subsequent change in behaviour and practices that often don't cost anything at all - at least not in monetary terms.
- Donors and partners are interested in a continuation of defenders' work. They will prefer to work with an organisation which recognises security issues instead of running the risk of an end to their work and a potential loss of their investments.

"If we pay so much attention to security we won't be able to do what is really important which is working with people and we owe it to them."

Reasoning behind the stereotype

Our own security and well-being does not impact our ability to help others. Our security and well-being are irrelevant to those we work with and for.

Responses to overcome resistance

- Security is a very individual concept and requires every individual to make decisions of the risks acceptable to them. Being sensitive to our security is part of our resistance against those who want to harm us for the legitimate work we do. We are much less able to take care of others if we do not take care of ourselves.
- If we care for ourselves and our security, we will be better prepared to care for those around us.
- People run risks by entrusting us with their cases and if we do not work on our security, it will affect them too; they might choose to trust another organisation that has adequately planned its security and is thus also giving more security to other people.

"We don't have time as we are already overloaded."

Reasoning behind the stereotype

It is impossible to find time in the work schedule.

Responses to overcome resistance

- It's a false distinction to think about security and well-being 'versus' our work. Security and well-being will make our work more sustainable. It is strategically more effective in the long term to make this space.
- Security management does not have to take much time. It's often just about small changes in our day-to-day work.
- In the long run, we will save time responding to emergencies if we are prepared in advance, and moreover, will have to deal less often with the physical, emotional and economic consequences of emergencies that affect us as human beings and organisations.

"The community is behind us: who would ever (dare) hurt us?"

Reasoning behind the stereotype

We are part of the community. The community is not fragmented, does not change either in members and opinions. The community cannot be influenced.

Responses to overcome resistance

- The community is not homogeneous and is also made up of those who might be negatively affected by our work.
- Under pressure, sometimes even those who want to support us can turn against us.

"In our village, the authorities have shown understanding and collaboration."

Reasoning behind the stereotype

Local authorities are not affected by our human rights work and will not change their minds. There is no hierarchy between national and local authorities.

Responses to overcome resistance

- Organisational historical memory will have examples of local authorities opposing human rights work when their tolerance limits have been exceeded.
- Local authorities have to implement orders from above. Authorities are made of people who might have an interest in protecting aggressors.
- Political contexts change.

Improving the Positive Impact of Your Security Measures and Reducing Possible Negative Impact: The Do-No-Harm Approach

Changing our practices regarding security can have both positive and negative impacts. As we build new security practices, it is worthwhile considering how we can enhance the positive impact on security for ourselves and others, while at the same time monitoring and attempting to reduce any negative impacts that these might cause.

We must begin from the perspective that as human rights defenders at risk, we are often operating in a context characterised by conflict. This conflict may be armed or unarmed and the violence to which we are subjected may be direct physical or armed violence, or may be economic, gender-based, institutional, structural, economic, psychological, etc. At times, activist communities are affected by conflicts within organisations, communities or movements. At the very least, we are rarely free from dynamics of privilege (related to gender identity, sexual orientation, race, religion, ethnicity, language, socio-economic status, etc.) and other forms of structural violence.

When we begin to adopt new behaviours relating to security, there can be some unintended negative consequences which affect these conflicts as a result. This doesn't mean that changing our practices is a bad idea – rather, it's just a good idea to be aware of these potential negative consequences, so that we can make truly informed decisions.

To achieve this, it is useful to engage with the **Do No Harm (DNH) Approach**.[21] It assumes that all our actions and behaviours lead to consequences, both positive and negative.

Actions + Behaviours = Consequences.

In the context of conflicts both internal and external to the group, our actions and behaviours can create additional **division** between people (hence worsening the conflict) or additional **connection** between people (relieving the conflict). Below, we consider some of the ways in which our actions and behaviours can have positive or negative effects on these conflicts when we implement changes to our security practices.

Actions and resources

We understand actions as everything we do and bring into an existing situation, including the resources obtained, used, and transferred in the course of your work and while implementing your security practices. Resources for security and well-being are often considered to be valuable and access to them may be limited. As you expand the actions and resources you engage with for security within your group or organisation, what might be the impact of these resource transfers on yourself, your allies and your opponents?

There are some potentially negative consequences to be aware of here, and these could easily develop into serious security issues. Four ways in which this can happen are:

21 For more, see CDA Collaborative, Do No Harm http://www.cdacollaborative.orgprograms/do-no-harm/

1 Competition vs. inclusivity

Supplying resources (such as training, computer hardware or well-being resources) only to selected individuals within a group might increase already existing tensions or create new ones. On the other hand, being inclusive about using and sharing your resources might help to connect people and strengthen feelings of inclusivity. If resources cannot be shared among all members of the group, it's important to have open communication as to why this is the case (perhaps due to higher risk levels of the individuals in question) and obtain the support of the group for this decision.

2 Substitution vs. appreciation

Adopting new practices or implementing new resources can mean that old practices, traditions or even people's roles are replaced or pushed aside. It is important that existing strategies and resources be recognised and replaced only when justified and in a way which respects the efforts which were put into them.

3 Selectivity and power relations

The members of the group who receive any extra training, attention, responsibilities, etc., can, through their access to new knowledge and resources, also gain more informal or formal 'power' or influence within the group, which can aggravate existing tensions or lead to new ones. By contrast, where possible, including the whole group or organisation can enhance acceptance of security measures and reinforce a sense of unity in the whole team.

4 Standard of living and working

This is particularly relevant in the case of staff members and volunteers. Who gets which training? Who gets paid for which activities? Who benefits more from security practices or suffers more burdens in everyday life and work? Who has what access to communication due to living in rural or urban settings? How can these dividing differences be bridged?

Behaviours and implicit ethical messages

When building our capacities and adopting new practices, we ought to also be aware of our behaviours, how they change, and how this may impact others. Our behaviours send non-verbal, implicit messages to our fellow activists, colleagues, team, organisation, allies and adversaries. The interpretation of these messages can, like with our actions, lead to further connection or division within the group.

It is good to consider each of our new practices and the potential messages they send to those around us, and where possible, seek to verify them. Below, we explore four common ways in which our behaviours can lead to increased connection or division within the group.

1 Cultural characteristics

One 'lens' through which others interpret our behaviours is, of course, culture. In multi-cultural environments, it's a good idea to consider how new security practices may be interpreted through this filter. For example, notions such as privacy, or the value of certain resources or social traditions, or a means of decision-making often vary greatly between different cultures. Be sensitive to your cultural surroundings and check whether the new security measures you take are being interpreted in a way that doesn't cause offence or division.

2 Different values for different lives

This can be especially relevant in groups and organisations which are of mixed nationality or background and wherein differing levels of 'expertise' – occasionally reflective of social class structures – are present. If certain groups or members are not included in the emergency plan of their organisation, they might interpret this as a sign that the organisation does not care as much about their security. Some international organisations, for example, do not reflect and plan for an evacuation of their local staff in an emergency, and focus only on their international staff. This can send a message that the well-being of some staff is more valuable than that of others. Furthermore, the importance of security awareness among administrative staff, cleaners and so on is often overlooked: consider who will pick up the telephone in order to receive an emergency call, or is most likely to recognise potential security indicators in the building? An inclusive approach not only allows for more cohesion and ownership of security measures in teams, but also to improved security for everybody.

3 Fear, tension and mistrust

Adopting new security measures can also be interpreted as communicating a lack of trust of and among colleagues, fellow activists or other stakeholders. For example, encrypting your calls over the mobile network could be understood as stating that you mistrust your regular telephone service provider; similarly, being less readily available for certain dangerous activities can lead to increased mistrust among fellow activists. As such, it is important to simply clarify the reasons for your new security measures and the logic behind them in a frank, open and honest way. Listen to feedback and commentary from those around you to see whether there are any consequences which can be avoided or worked on, and do what you can to maintain trust in both directions. In the case of adopting radical new security measures and thereby potentially attracting negative attention from adversaries or neutral parties – such as through encrypting communications, and being noted by telephone or Internet Service Providers – consider using old or common methods in parallel to new ones in order to lower suspicion.

4 Use of resources

Any new resources – such as computer hardware or software, training, vehicles, access to psycho-social support, etc. – which are made available for increased security – should be used responsibly by those who have access to them. Group or staff members who do not have prioritised access to such resources can get the impression that they are used by their colleagues for their own personal benefit if their purpose is not shared within the group or organisation. This exclusivity can send out the message that the one who is in control of resources can use them for his or her own purposes without being held accountable.

In order to analyse your behaviour and the messages in your own security practices, it may be useful to draw a table such as the example in **Appendix F** and consider the examples given before filling it in for yourself.

We should consider our practices in light of these concepts and talk about them in a safe space with our friends, family and colleagues to try to fortify their positive effects on our relationships, and lessen their negative effects. Reflecting on our security framework in terms these questions might prevent us from producing new kinds of threats scenarios by our security set-up by creating more connecting activities and behaviours, which benefit everybody's security.

Conclusion

Through **Prepare**, **Explore** and **Strategise**, we have charted a path from defining security for ourselves and creating a space for security within our organisations, through carrying out an analysis and diagnosis of our security situation, and planning for maintaining and improving our security in the course of our work as human rights defenders.

How you will implement this idealised series of steps depends greatly on the nature of your work, and those with whom you work. It is important to keep in mind that they represent a cyclical process of evolution, and constant reassessment of our situation and updating of strategies and plans is ideal.

While the three Sections in this manual have focused on the management of a security capacity-building process in a group, the next step is to get to know particular tools and tactics which you can put into practice for increased security during different aspects of your work.

In **Section IV | Act** you can find tools and tactics sourced from a community of human rights defenders, trainers and experts on security and well-being which can be implemented in particular, high-risk activities for human rights work.

Further Reading

- **CAPACITAR Emergency Response Tool Kit**
  A response to the trauma of Hurricane Katrina, the kit includes simple basic practices taught by Capacitar to empower people to deal with the stress of challenging situations.
  http://www.capacitar.org/emergency_kits.html

- **CDA Collaborative, Do No Harm**
  A framework for analyzing the impacts of aid on conflict and for taking action to reduce negative impacts and maximize positive impacts.
  http://cdacollaborative.org/cdaproject/the-do-no-harm-project/

- **Insiste, Persiste, Resiste, Existe: Women Human Rights Defenders' Security Strategies**
  The report brings together the voices of women human rights defenders from

all over the world on combating violence and discrimination in complex contexts – in situations of overt or hidden conflict, organised armed violence as well as rising fundamentalisms.
http://kvinnatillkvinna.se/en/publication/2013/04/18/insiste-persiste-resiste-existe-2009/

- **Integrated Security: The Manual**
  This manual covers all aspects of an activists work and life, from health and personal networks to secure working spaces. This manual shows how you, a human rights defender, facilitator, international human rights organization, supporting donor or organization working in emergency and development contexts can arrange Integrated Security Workshops.
  http://integratedsecuritymanual.org

- **New Protection Manual for Human Rights Defenders**
  The purpose of this manual is to provide human rights defenders with additional knowledge and some tools that may be useful for improving their understanding of security and protection.
  http://protectioninternational.org/publication/new-protection-manual-for-human-rights-defenders-3rd-edition/

- **Security in-a-Box: Tools and Tactics for your Digital Security**
  A digital security toolkit for activists and human rights defenders throughout the world.
  https://securityinabox.org

- **Security to Go: A Risk Management Toolkit for Humanitarian Aid**
  A simple, easy-to-use guide for non-security experts to quickly set up basic safety, security and risk management systems in new contexts or rapid onset emergency response situations.
  https://www.eisf.eu/library/security-to-go-a-risk-management-toolkit-for-humanitarian-aid-agencies/

- **Workbook on Security: Practical Steps for Human Rights Defenders**
  A step by step guide to producing a security plan – for yourself and/or your organisation following a systematic approach for assessing your security situation and developing risk and vulnerability reduction strategies and tactics.
  https://www.frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk