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.