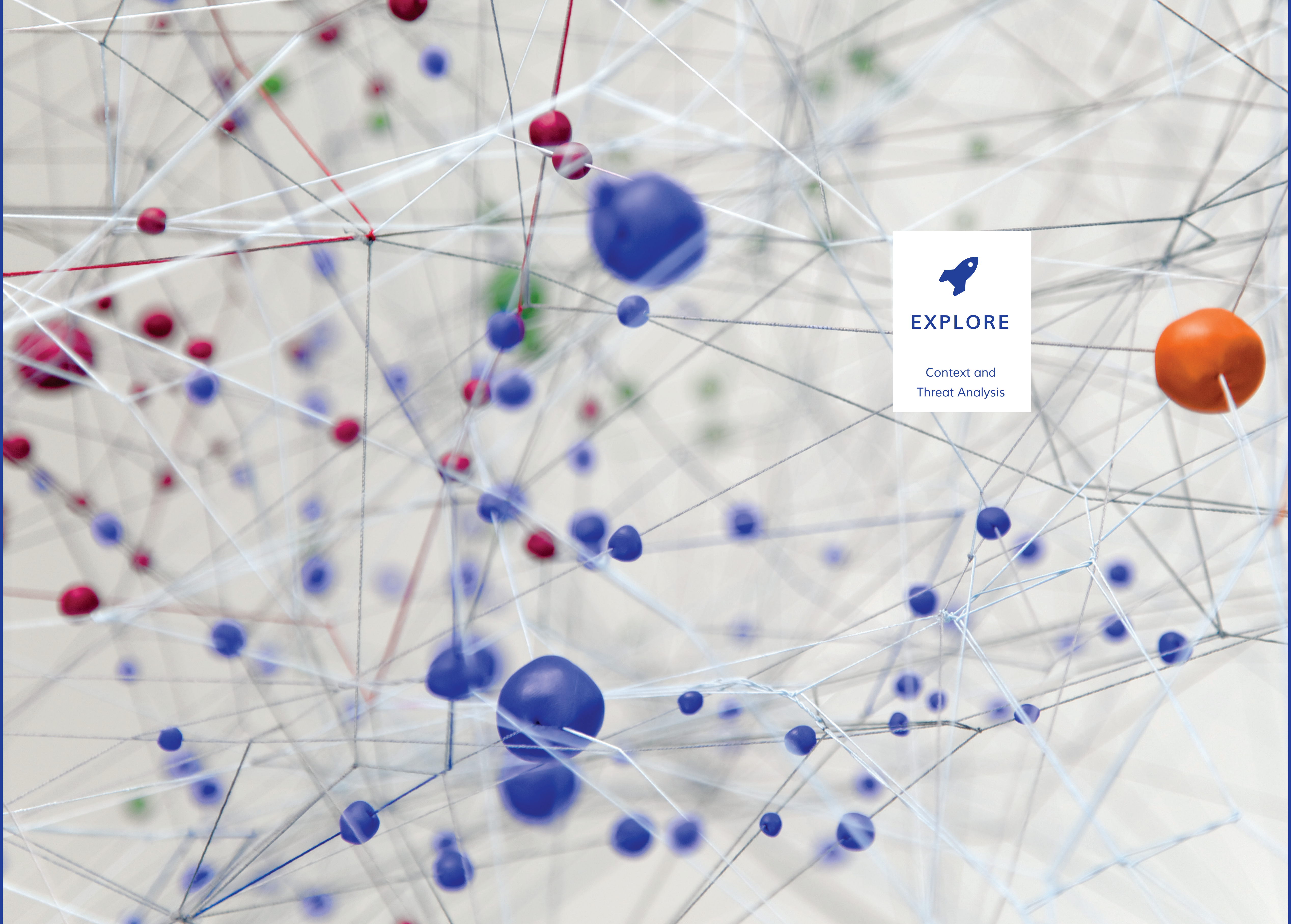


EXPLORE

Context and Threat Analysis

II Explore

Context and Threat Analysis

Contents

Introduction

In this Section, we will analyse the context in which we carry out our work in the defence of human rights. Creating and maintaining a systematic analysis of our political, economic, social, technological, legal and environmental context allows us to better understand the threats we face, prepare ourselves to deal with these threats and maintain our well-being as we pursue our goals.

Threats, in this case, refer to **any potential event or occurrence which would cause harm to ourselves or our work.**

This process is sometimes also referred to as threat modelling or risk analysis.
The more time we can make for this context analysis, the better we will understand our surroundings and the better prepared we will be to perceive and respond to threats to our security and well-being.
The tools for context analysis explored in this Section, therefore, can and should be woven into our existing processes for strategising and planning our work in defence of human rights. You may already be familiar with a number of these tools and use them without being explicit or especially organised about it. However, being more systematic about it will help you make a more complete 'diagnosis' of your security situation, and perhaps challenge some assumptions you may have about it.

In Explore, we will:

- propose a series of steps for carrying out **context analysis**
- carry out a simple exercise for understanding the **socio-political trends** around us
- map out our **vision** and the **actors** around us in this context
- create an **inventory of our information** as a resource for our work, and understand the threats to it
- **recognise and analyse indicators** which tell us more about our security situation
- identify and analyse the **most relevant threats** to our security.

1

Overall Framework for Context Analysis

Effective security practice is based on good knowledge of the kind of threats we face as a result of our work and the possible harm those threats represent. But how easy is it to accurately identify all the threats that might negatively impact our well-being and ability to achieve our goals? To answer this question, we must consider two key factors.

Evolving threats

It is important to recognise that threats are constantly changing, sometimes very rapidly. As we go about our lives and work, so do our allies and our opponents. With advances and setbacks, as well as changes in the political, economic social, technological, legal and environmental contexts in which we work, the range of threats that we face shifts and changes. The threats that we prepare for today may be irrelevant in a month, and the key to success is remaining agile and reviewing and refining our security practices on an ongoing basis.

In reality, this isn't necessarily a very alien concept to us. We regularly carry out context analysis to make decisions about our security in our day-to-day life. The only difference here is that we are being more deliberate and organised about this process. This helps us avoid taking security precautions just our of habit or based on hear-say, as we may find that changing circumstances render them ineffective.

Context analysis helps us to understand more clearly the threats we might face as a result of our work. It comprises a series of familiar steps and perhaps some new ones. The steps we will follow are outlined below – you may find that you are already carrying out some of them.

1 **Situation monitoring and analysis** Observing the overall trends (political, economic, social, technological, legal or environmental) which are relevant to our work and taking note of any developments relative to our security. a simple example of this is reading the newspaper on a daily basis although there are a number of other sources of security-specific information.

2 **Establishing our vision and activities** Based on the above, we reflect on what change we envision in our society and what strategies will help us implement this change. Many human rights defenders will be familiar with the exercise of identifying a problem we want to fix in our society, and a strategy for carrying that out.

3 **Actors and relational mapping** Creating and maintaining an inventory of all the people, groups and institutions who will be or may be affected by our action, including ourselves, our allies and opponents.

4 **Information mapping** Taking account of our personal and professional information, and making sure it doesn't fall into the hands of the opponents we have identified. A simple example would be distinguishing your financial documents from other documents at home, and deciding to store them in a safer place.

5 **Security indicators** Taking note of occurrences which are out of the ordinary which may indicate a change in your security situation, and analysing any trends to be noted which may impact your strategy. A simple example would be noticing an increase in thefts in the area where you live, and an acknowledgement that it may affect your security too.

6 **Threat identification and analysis** Attempting to drive off the danger by pretending to have greater power than one actually does. As human rights defenders, we often threaten to expose and publicise threats of violence so as to publicly embarrass our adversaries.

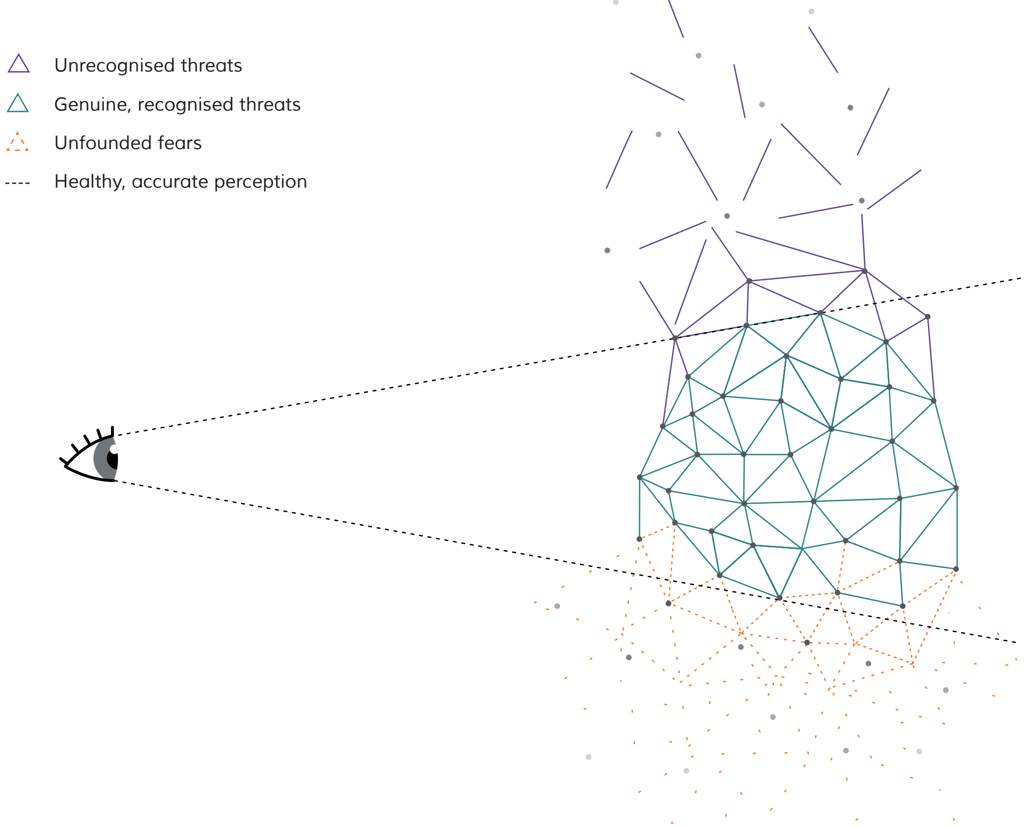
7 **Security planning and tactics** Based on this analysis, you identify and take concrete measures to improve your security, such as buying new locks for your doors or CCTV cameras. We will look at this in more depth in Section III | Strategise and Section IV | Act.

These steps do not represent one-off activities, however, and must be regularly repeated and woven into our ongoing strategic planning in order to be effective.

Analysis and perception

It may be tempting to consider this kind of analysis as scientific or objective. However, at this point it is useful to remember what we learned in **Section I | Prepare**. By definition, our **perception** of threats is sometimes challenged, limited or flawed. While there may be many threats of which we are aware, there may also be some of which we are not aware. Such **unrecognised threats** are particularly likely when we are working in new environments with limited understanding of our surroundings, or where our opponents are actively concealing threats, such as electronic surveillance. Anxious emotional reactions such as denial, fatalism or minimising effect might also result in us failing to recognise potential threats.

Perception of Threats


△ Unrecognised threats
△ Genuine, recognised threats
△ Unfounded fears
---- Healthy, accurate perception

It is also possible for us to err in the other direction, and focus on threats which are not in fact likely to harm us or our work. Such **unfounded fears** may result from misinformation from our opponents or from anxious emotional reactions, possibly related to past traumatic experiences. Still, it is possible and useful to make adequate security decisions based on the limited and one-sided information available. Experience brings us insight and our intuition mostly guides us in the right direction. While our opponents develop new tactics and work to confound our security practices, the challenge that we and our allies face is to **reduce the number of unrecognised threats and unfounded fears**, thereby building a more accurate picture on which to base our security practices.

Starting from the acknowledgement that our perception of threats may be flawed, it's a good idea to think in advance about where our blind spots may be and devise strategies for checking our perceptions with people we trust. We will return to this in **Exercise 2.6b**, where we pose some questions which may help with this.

Our perception can become more accurate if we carry out research and analysis. In the rest of this Section, we chart a path of self-exploration, starting with our own vision for socio-political change, continuing to a survey of the universe in which we operate alongside our opponents, allies and other parties; an inventory of our existing resources, assets and behaviours, and an accounting of what we perceive as security indicators in our context (i.e. the precursors to threats).

The knowledge gained from the above exploration is helpful in creating and maintaining a prioritised list of potential (and actual) threats, their likelihood and severity, the potential (or actual) perpetrators and their abilities and motivations, any existing mitigations we (or our allies and others) might have in place, as well as potential next steps in further minimising these threats to our well-being and success.

As we start this exploration to identify and mitigate the threats we face, it is important to be mindful about not creating or further encouraging unfounded fears. This can be avoided if we keep in mind the role our perception and behaviour play, and work to create a healthy space to deal with these challenges. Namely we need to encourage a self-aware individual mind-set and healthy communication in teams and organisations, as explored in **Section I | Pepare**.

It is equally important to remember our own limitations in terms of time, stress and resources. This helps us determine a realistic, tangible and manageable task in identifying, prioritising and analysing threats.

In the next Chapter, we will begin by looking at the political, economic, social and technological landscape in which we operate as human rights defenders, and how that may impact our security.

2

Situation Monitoring and Analysis

We will begin this process with the broadest kind of analysis of our context: observing the political, economic, social, technological, legal and environmental developments in society which are relevant to our work, and may impact our security situation.

In the course of our activism in general, it is likely that we engage either informally or formally with some situational monitoring and analysis: that is to say, analysing whatever sources of information are available to us regarding the **political, economic, social, technological, legal and environmental developments** in our society. We may do this by simply reading the newspaper every morning or talking to trusted friends or colleagues about their observations. It can also comprise more complicated or sensitive tasks like carrying out our own investigations and research. Through this process, the information we obtain naturally informs the decisions we make and the strategies, plans and actions we take as activists.

However, in carrying out and sustaining an ongoing situational monitoring, it is important to consider the **sources** of our information: is the media a reliable source of objective information, or do we have to diversify our sources? Colleagues, friends and partner organisations, as well as academics, experts, friendly authorities and embassies, security-related email lists, travel agents among others, can also be rich sources of contextual information which may be relevant to our strategy and our security.

Carrying out a more in-depth and deliberate monitoring and analysis of our situation on a regular basis is also a great way to reflect upon our security situation. It helps us to situate our work and our strategies within ongoing local, regional, national and global developments, and identify those which may point to a potential change in our security situation.

Situational monitoring and analysis can be thought of as the 'engine' of our security planning, from which we can identify the **key developments** which will impact our strategy. Examples of key developments include:

- the appearance of new actors (such as newly elected politicians)
- the emergence of new forms of electronic surveillance or ways to avoid it
- a change in the discourse of key actors regarding how they view our work.

Regularly analysing developments such as the above with trusted partners is a key security practice, and also helps us to **check our perceptions** so that we are less likely to suffer from **unfounded fears** or **unrecognised threats**.

There are a number of frameworks which can be used for situational analysis. Two common types of situation analysis which are often undertaken in the context of strategic planning are a PESTLE (Political, Economic, Social, Technological, Legal and Environmental) analysis, or a SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis. In the next exercise, we will carry out a brief PESTLE analysis and attempt to identify key developments from the last year of which we should be aware.

2.2 Exercise

Situational monitoring: quick PESTLE analysis

Purpose & Output

This exercise helps us consider the ways in which we already carry out a situational analysis, and briefly consider some of the dominant trends and developments in the last 12 months which may impact our security.

Input & Materials

Writing materials

Format & Steps

Alone or in a group, consider and take notes of your answers to the following questions:

1. How do you currently carry out situational monitoring and analysis? What spaces do you have for discussing ongoing developments in society?

2. What are your sources of information for this?
   - Make a list of these, and for each one, take notes on their strengths and weaknesses in terms of the quality of information they offer. Are they objective or biased?

Format & Steps

3. Consider what has happened locally, regionally and internationally in the last 12 months and make a list of 5 to 10 developments you consider important. You may not need to categorise them, but be sure to consider:
   - political developments
   - economic developments
   - social developments
   - technological developments
   - legal developments
   - environmental developments.

Note: If you can't think of new developments in the last 12 months, consider generally salient characteristics.

4. Could any of these developments impact your security, directly or indirectly? If so, how? Did you suffer any attacks or accidents in the last year? How did they relate to these developments?

3

Vision, Strategy and Actors

Carrying out a situational analysis, as above, often highlights the trends in our society that we see as negative or unjust. In this context we strive to affect changes in our society which can include civil and political rights and economic, environmental, gender and social justice, among many other forms of justice. As human rights defenders, we are accustomed to identifying injustice and responding to it. It is important, however, to have a defined vision of the change we wish to engender and a strategy to achieve it. Based on this strategy and an understanding of how we will implement it, we can identify the threats we face and build a comprehensive and appropriate security plan.

Thinking critically about our strategy becomes even more important if and when we act as a group or an organisation. Being internally transparent and open about the changes we want to achieve and the strategies we use can also prevent difficulties and conflict within the group and those outside it.

Establishing our vision and activities

Identifying a problem we want to resolve is often our first step as human rights defenders and this is hopefully accompanied or followed by envisioning the successful result of our work. If you don't have an already established vision, answering the following questions may help:

- What is the problem, or the problems, that you hope to address?
- What change do you wish to see?
- How would your community be different afterwards?
- What would be different about the relationships between people if you succeed?
- Who are the other individuals, groups, institutions, etc. involved in this issue and how do they react to your activities?

Activity mapping

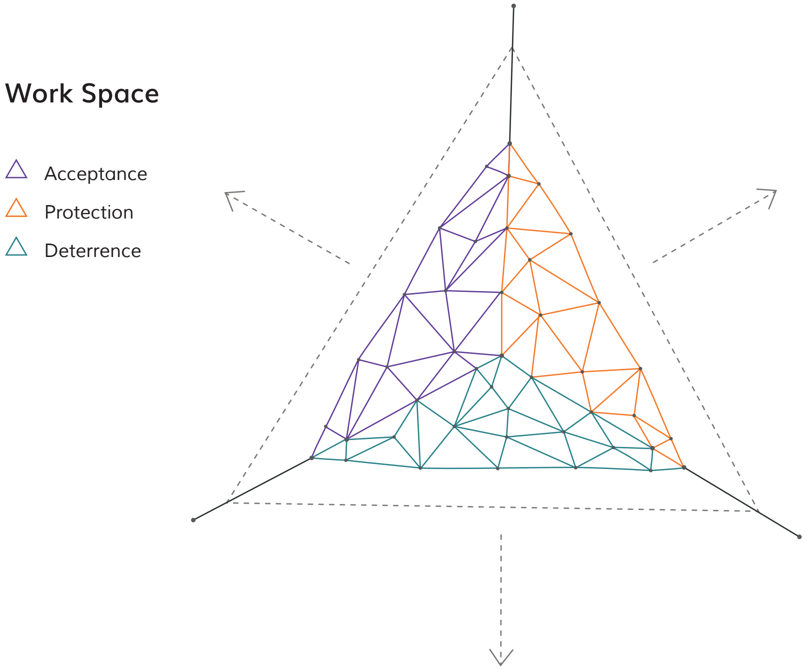
Once we have established our vision, we must consider the methods we can employ to realise it. We may carry out very diverse activities as individuals or organisations in order to achieve our goals. What are your 'areas of work' or the activities you carry out?

It is important to explicitly list them and consider, in the first instance, whether or not they are appropriate for achieving the objective we have set. Our work does not take place in a vacuum, but rather in a rich and diverse context, often with some characteristics of conflict. Our activities are our 'interface' with this conflict and with the State and the society that we are trying to influence; they are our means of attempting to change the situations, the perceptions and behaviours of a diverse set of actors (individuals, institutions and organisations) around us. Some of these actors will benefit from, believe in and support our activities. Others, however, will feel that these activities are not in their interest and will attempt to close our space for work.

Actor mapping

Building your strategies helps to identify the entire range of actors (individuals, institutions, organisations, etc.) who are the 'players' in the current situation. They may be working to sustain or challenge the status quo, or neither, or occasionally both. Identifying all the actors means you can prioritise appropriate actions for your engagement with each type of actor, such as how to shift their opinions of your work, change their habits or stop them from behaving a certain way. Keep in mind that your opponents as much as your allies develop their own strategies and actions based on the perception they have of your position and activities. This perception might differ from your own.

Therefore, understanding the actors involved and spending time on collecting information and reflecting on dynamics is crucial to your security planning. Deeper knowledge of our allies and opponents also helps us decide which acceptance, deterrence or protection strategies to employ in order to maintain our socio-political space for working, which are discussed further in **Section III | Strategise**.



One helpful way of starting this process of actor mapping is to carry out a visual brainstorm of all the the actors in the field and the nature of the relationships between them, as demonstrated in the following exercises.

2.3a Exercise

Visual actor mapping–part 1

Purpose & Output

The idea of this exercise is to begin a process of visualising yourself, your group or organisation,and your relationships to the other actors around you, including direct, indirect and potential future connections.

In this part, we suggest that you focus on brainstorming who the actors around you are and the intensity of your relationship with them (direct, indirect, or potential).

In the next step of the exercise, you will extend the visualisation or map to include the types of relationship you have with them.

Input & Materials

If you want to carry out this activity in a group, you will need:

- butcher-block or flip-chart paper
- coloured markers or pens
- sticky-notes / Post-its.

Format & Steps

Written/drawn visualisation

In this exercise we suggest that you use sticky-notes or post-its, each with the name of one actor in your context, to visually map them and the relationships between them.

1. Start with yourself or your organisation as an entity and brainstorm and identify as many actors related to your work as possible. This can include individuals, groups, organisations or institutions. Consider local, regional, national and international actors where necessary.
2. Once you have identified as many of the actors as you can, place them on the wall or sheet, with yourself (and/or your target group, if they are identifiable) in the centre.
3. Consider the following categorisations for these actors:
   Direct: People, groups, organisations, institutions that have direct contact with you on the issue you are trying to impact. For example, you probably have a direct relationship to the tar-

Format & Steps

get-group you work for, and some entities directly opposed to your work who directly challenge or confront you.

You may also want to include members of the community around you including your family and friends who may support or oppose your work in one way or another.

- **Indirect:** These can include people, groups, organisations or institutions that are one step removed from you. In the example above, if your target group has a direct relationship with you, they may be in direct relationship with others. These become indirectly connected to you.
- **Potential/Peripheral:** People, groups, organisations and institutions which relate to the issue, but with whom you don't (yet) have a connection or relationship. Examples of these include international bodies which are supportive of your issue, but aren't (yet) active in your context.

Note: Actors and information

Although it may not have occurred to you, you may want to include actors on whom you rely to manage your information and communication. These can include:

- your telephone service provider
- your internet service provider
- social media account providers
- email account providers.

We will explore these actors in more detail in the next exercise.

Remarks & Tips

In the next and subsequent Chapters, we will expand our knowledge of these actors and use them to build our analysis of threats. Once you have finished this exercise, it's a good idea to keep a list of these actors for future reference and elaboration.

Expanding our knowledge of actors

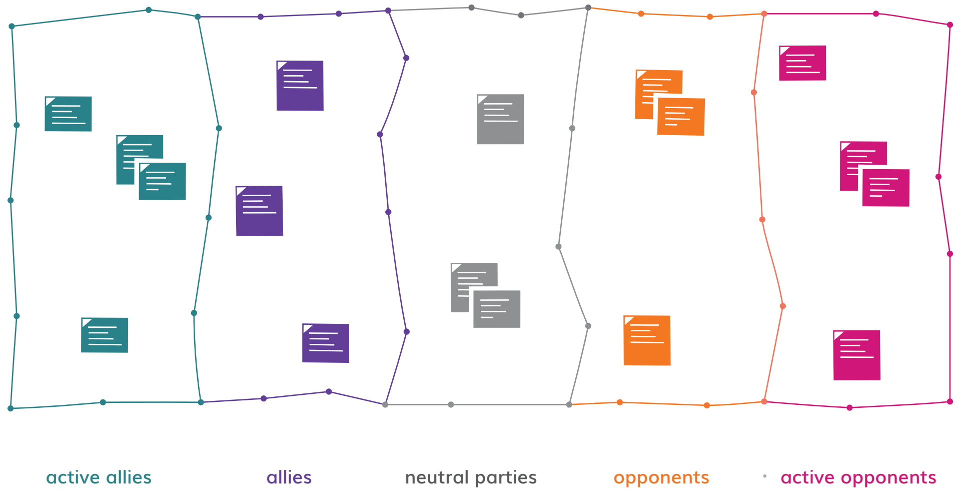
Once we have established the actors in our environment, it is helpful to categorise, to the best of our knowledge and ability, the nature of the relationships between ourselves and these actors, especially their stance regarding our vision, their interests and the amount of resources at their disposal.

We might roughly categorise the actors into three groups:

- **Allies:** these are actors with strategic alignment to our goals. The strength and longevity of their support may fluctuate over time. They may include fellow human rights defenders and organisations, the community we work for, friendly elements of the State, embassies, and our friends.
- **Adversaries or opponents:** these are actors whose strategic interests are opposed to ours, or somehow oppose our goals for various reasons. The intensity of opposition or disengagement may vary with changing circumstances. For some human rights defenders, especially those working on gender and sexual rights issues, these may also include family members.
- **Neutral parties:** these are actors who neither support nor oppose our cause. However, their role may change depending on the changing situation.

It may be useful to imagine or visualise these actors as a **spectrum**:

Spectrum of Allies



The ‘spectrum of allies’[8] demonstrated above is often used in an action campaign design, in order to identify the key sectors of society which we wish to influence so that they move in the direction away from the position of active opposition and towards the position of active alliance. This can also be used in security planning and promoting acceptance and tolerance of our work among different elements of State and society.

Mapping relationships between actors

The next step in our visual actor mapping exercise includes analysing, identifying and specifying the nature of relationships between actors. This step is particularly useful in identifying actors whose motivations may lead them to threaten us or our work, as well as allies who can be relied upon to help us work more securely.

2.3b Exercise

Visual actor mapping–part 2

Purpose & Output

This exercise builds on **Exercise 2.3a** by denoting relationships among the actors in the map, identifying the allies, opponents, and neutral parties.
The resulting map can then be used to identify and analyse specific actors in your context who may represent intentional (or unintentional) sources of threats.

Input & Materials

- A basic actor map (from the previous exercise)
- Paper and coloured markers or pens
- Coloured dot stickers

Format & Steps

Written/drawn visualisation
Considering all the actors you have brainstormed so far:

1. Denote actors based on the nature of their relationship to your work (ally, adversary, neutral, unknown). This can be done by assigning a coloured dot to each type of actor, different coloured post-it notes, or different locations (allies on the left, opponents on the right, neutrals in the middle, etc.).
2. Draw a circle around each actor on the map. Its size can correspond to its **power and resources** in the socio-political context (see legend below).
3. Starting with yourself on the map, you can make connections to any actor with whom you have a relationship.

Use the legend on the next page to represent the different types of relationships that exist between the actors on the map.

Examples of relationships to include here are:

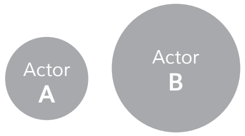
- Close relationships: where actors enjoy a positive relationship with each other.
- Alliances: where actors coordinate their activities with one another and act as one.
- Weak or unknown relationships: relationships with little contact, or where the nature of which is unknown.
- Conflict: where two actors have an antagonistic relationship with one another.
- Violent conflict: where the relationship is characterised by physical (potentially armed) violence by one or both parties.
- Compulsion: where an actor has power over another one and can make them do something, e.g. a paramilitary group which is controlled by the armed forces.
- Interdependent: where two entities are bound to each other in some manner.

Remarks & Tips

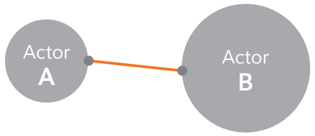
It is useful to periodically revisit and reflect on the map you created and make any additions, subtractions or changes that occur to you. Remember, it is important that this is re-evaluated and updated regularly, especially before a new action.

[8] Based on the “Spectrum of Allies” exercise from ‘Training for Change’ . A good deepening on engagement with actors from these categories can be found here: https://organizingforpower.files.wordpress.com/2009/05/allies-chart-new1.jpghttp://www.trainingforchange.org/tools/spectrum-allies-0

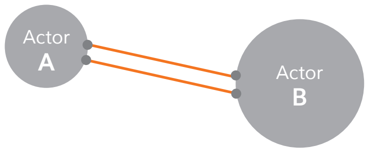
Legend[10]



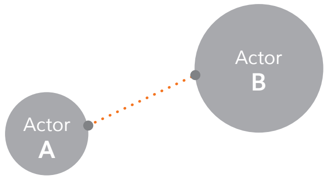
Different sized circles represent differences in power



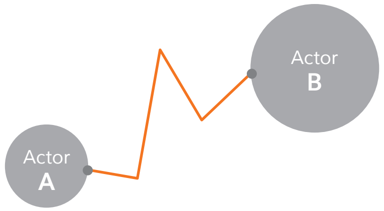
A solid line represents a close relationship
You can also 'break' the line (by crossing it in the middle) if there is a broken relationship



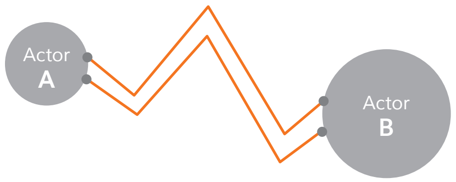
A double-line represents an alliance



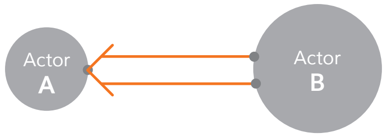
A dotted line represents a weak or unknown relationship



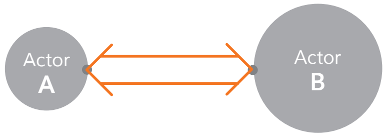
A jagged line represents conflict or a bad relationship



A double jagged line represents violent conflict



A double-line with an arrow represents domination, control or compulsion (where one actor acts under orders of another)



A double-line with an arrow in both directions represents interdependence

[10] Adapted from KURVE Wustrow (2006) Nonviolent Conflict Transformation. A Training Manual for a Training of Trainers Course. Centre for Training and Networking on Nonviolent Action KURVE Wustrow e.V., Wustrow. (pdf: http://www.trainingoftrainers.org/), pp.45-46.

Additional actor information sheet

For each of the allies and opponents (but prioritising the active ones), you can elaborate on the nature of their relationship to your work, and create an information sheet that provides further information on their motivations, their interests, the history of their relationship with you and their resources (material, financial, relational or other).

This information sheet will help you to:

- identify the underlying interests and relationships that motivate their stance. Why are they 'with' or 'against' you?
- identify the resources and strategies they possess and employ which they may use to help or hinder your work. Reflect also on their position within the broader socio-political context and which privileges and resources they might draw from that position.

It is important to note that these motivations and resources will change over time. This analysis should be updated regularly as new information emerges. Furthermore, it's very important to consider sources of information about this trustworthy: be it through personal contact, informal networks, local media or other.

Once you have completed a visual actor map for the first time, it may be useful to transfer the information to another format where it can be regularly updated according to your situational monitoring and analysis, and the ongoing changes in your activities.

In the next segment, we will consider the importance of information and how it moves between ourselves and the other actors on the map. In addition to exploring why we should pay attention to our own information, how we generate it, use it, share it, store it, etc., we will also explore what measures to take to protect our communication and information.

4

Understanding and Cataloguing our Information

This Chapter involves understanding what ‘information’ actually means in relation to our activities and goals as activists. The importance of information management cannot be underestimated, especially given the growing use of digital technologies in the context of defending and promoting human rights. While these tools offer us great potential for communicating, researching, organising, and campaigning, they are also a key target for our adversaries seeking to place us under surveillance, gather information or hinder our work.

When we talk about ‘information’ in the context of our work, we refer to many things, such as:

- The outcome of the work we are doing; such as a report, a database of human rights violations, images, voice and video recordings.
- Operational information that helps us do our work; such as our text messages during an action, our files and progress reports and other office information and communication, including financial, human resources and strategic organisational documents.
- Personal information that identifies who we are both as members of an organisation, as well as other personal or professional affiliations.
- Data generated by our use of digital devices as we work, or ‘meta-data’, which can be used to track our movements or monitor our relationships.

This information can be stored and communicated in many ways: on paper, on our computers, on mobile phones, on the internet, on file servers, various internet services and social networking outlets. Taken together, this information comprises one of the most important assets any of us (or any organisation) has. As with any asset, we are best served when we are sure that this asset is properly cared for so it doesn’t accidentally or maliciously get lost, corrupted, compromised, stolen or misused.

In caring for our own security, we need to care for the security of our information. Information about us, our activities and our plans can be very useful to our opponents and with the increasing use of digital devices and social media, it is imperative that we make sure we remain in charge of who has and controls our information. Surveillance and information gathering have always been used to plan attacks against human rights defenders, and such invasion of the right to privacy could itself be considered a form of (often gender-based) violence.

Common threats to HRDs’ information

Data loss Due to poor computer hygiene, malware infections, power cuts or ageing hardware, computers and other devices occasionally cease to function causing us to lose our data.

Compromised accounts Sometimes, our passwords or ‘secret questions’ are not very difficult to break, or we are subjected to phishing attacks (which can be random or targeted for us especially) and unknowingly hand them over to a third party, who gains access to our email or social media accounts.

Device confiscation or theft Computers and mobile phones are common targets for thieves. Furthermore, if we face acute risk, our offices and homes may be raided by State or non-State actors and computers, mobile phones, hard drives, USB keys and servers could be ‘confiscated’ or stolen for analysis.

Device inspection at checkpoints Sometimes we may have our devices temporarily confiscated while crossing borders or military checkpoints, where the data may be copied or the computer may be infected with spyware or have a hardware keylogger attached.

Information handover Internet service providers and the providers of the email and social networking sites that we use can also hand over our data to certain authorities if a legal request is made to do so. While they protect our data from some, they are more willing to hand it over to others, and this situation is constantly changing in accordance with business and political interests.

Surveillance and monitoring Data brokers, internet service providers, email providers and many other companies subject the general population to surveillance by gathering and aggregating details of our online activities. While in some cases this has the aim of merely targeting us with advertisements, it can also be used to identify particular minorities to which we may belong as a target for deeper surveillance.

Targeted malware Targeted malware is a growing industry: some State authorities and other groups invest in software which is designed to trick us into downloading it and later granting the attacker access to much or all of the data on our devices.

The security of our information is critically important and so protecting it can become a source of anxiety. An effective and up-to-date information security strategy can give us the peace of mind needed to focus on our objectives and carry out our work in a healthy way.

The first step involves a process of cataloguing, as much as possible, all instances or versions of our information. Creating a mental understanding of what elements exist in our own information 'ecosystem' will help us move away from perceiving 'information' as a vague mass of data, towards a better understanding of it as a tangible and important asset.

By cataloguing our information into various components and types, we can identify any potential situations and avenues where our information may be or may become vulnerable, as well as areas where we need to improve its safekeeping.

This process relies on the output of the previous exercises where we identified the 'actors' in our context, including ourselves, our allies opponents and currently neutral parties. We may refer back and expand the actor map with potential new actors identified through the information mapping process. The map will also facilitate understanding of the relationship between elements of our information and our allies and opponents and their intentions and abilities.

Next we look at some key concepts for understanding how to catalogue our information, followed by the 'information ecosystem' exercise which will help us generate a map of our most important information assets.

Categories of information

The first step to creating an information security strategy is to get to know what information we have, where it is, and how it moves from one place to another.

A simple way to start this cataloguing process is to think of the information in terms of what is primarily stationary (at rest) and information which travels (in motion). Examples of this may be financial information stored in a filing cabinet (information at rest) versus exchanging messages via mobile phone on an upcoming event (information in motion).

This distinction is used primarily as an organising principle to help with the categorisation process. It is important to remember that today much of our information is in digital form, and with increasing use of the internet and remote storage services (i.e. 'the Cloud'), much of the information we possess is at one time or another in motion. Similarly, due to the growing popularity of hand-held devices (such as smartphones and tablets), increasing storage capacity and the actual mobility of these devices, any information stored on such devices, although it may be digitally 'at rest', is actually moving in physical space.

It is worth repeating that under the above categorisation, our communications – such as emails, chats, text messages and phone calls are 'information in motion', and that this is extremely common, especially in the context of having near constant connectivity over the internet. Where this organising principle can become useful is when we decide what tactics to employ in order to better secure our information, as there are distinct ways of securing information at rest and information in motion.

Information at rest

Once we have established our vision, we must consider the methods we can employ to realise it. We may carry out very diverse activities as individuals or organisations in order to achieve our goals. What are your 'areas of work' or the activities you carry out?

It is important to explicitly list them and consider, in the first instance, whether or not they are appropriate for achieving the objective we have set. Our work does not take place in a vacuum, but rather in a rich and diverse context, often with some characteristics of conflict. Our activities are our 'interface' with this conflict and with the State and the society that we are trying to influence; they are our means of attempting to change the situations, the perceptions and behaviours of a diverse set of actors (individuals, institutions and organisations) around us. Some of these actors will benefit from, believe in and support our activities. Others, however, will feel that these activities are not in their interest and will attempt to close our space for work.

All of these can often provide a source of information about a person, a project, a movement or an organisation and for this reason, theft and confiscation of computers, phones, and memory storage devices are common tactics of human rights defenders' opponents.

When brainstorming a list of your 'information at rest', it helps to consider some attributes, such as:

- where they are
- who has access to them
- how sensitive is their content to you, your organisation or people mentioned in the document (e.g. witness or victim statements)
- how important it is to keep them
- how long they should be kept.

Information in motion

As mentioned before, many of the information assets we have (especially in digital form) are at some point transported from one place to another. Consider all the ways your information may be moving:

- the box full of documents you send to the archives via courier
- a phone call you make over the mobile network
- videos of an event you upload to a server online
- the contact information in your mobile phone as you participate in a protest.

In the examples above, we can see various ways our information is in motion: physical pieces of information travelling in physical space, or digital information travelling through the internet, or digital information (stored in physical devices) traversing physical space.

We should also pay attention to the different ways information can travel:

- **Transfer:** Whether during an office move, or when an attachment is sent to a colleague over the internet, or a backup of sensitive files is made to a server in another location, our information is transferred from one point to another.
- **Communications:** When we interact with our colleagues, allies, the public and indeed opponents, there is an exchange of information that takes place. Communication can take the form of announcing instructions from a loudspeaker at an event, or exchanging confidential information during a phone conversation, a video-call, an in-person meeting, emails, text messages and many others. Our communication contains lots of information about our intentions, the status of our action, and our plans and future activities.

To catalogue such information, in addition to the attributes mentioned for 'information at rest', you can also think about:

- how the information is transferred
- what physical or virtual routes it takes
- who may be able to access it along the way, or who would be interested in capturing it (consider your actor map)?

Digital forms of information

There are some unique attributes related to information which is in digital form worthy of consideration:

- **Replication:** Information in digital form is constantly replicated. During file transfers, email exchanges, uploads and downloads, and even when moved from one device to another, copies of the information are created, which for all intents and purposes are identical to the original. This is slightly different from the pre-digital era where it was possible (though at times difficult) to distinguish between an original piece of information (e.g. minutes of a meeting typed on a sheet of paper) and subsequent duplicate copies.
- **'Permanence' of information:** As noted above, once a piece of information is uploaded to the internet, the process of upload, transfer and download entails multiple occasions where the information is copied. It follows that our information may be retained somewhere as it is traversing parts of internet which we don't control (as often is the case). Copying and relaying happens as mail-servers, routers and intermediary locations make copies of the information to aid the transfer process, or for other purposes, depending on the intentions of whoever controls the devices. It is therefore important to understand that it is possible for a copy of a piece of information to be kept intentionally or unintentionally by one (or many) of these actors for a long time.

An example many people can relate to is a text message. These messages are sent from one mobile phone to another, but as they are sent, they pass through a number of cell towers and other infrastructure which belongs to the service provider. The service provider has access to these messages and will, in most cases, retain them for a period of time, regardless of whether you delete them from your telephone or not.

- **Metadata:** As computers and digital devices carry out their operations, a layer of 'metadata' is created. Metadata is information created about and by these processes themselves. This information accompanies the data itself, and sometimes it cannot be removed from the data. Examples of metadata include:
  - Your **IP address** which locates where you are connecting to the internet, and the IP addresses of the websites you visit.
  - the **location data** of your mobile phone as it moves from one point to another, **the unique identifying numbers of the SIM card and of the phone** (known as the IMEI number). It is generally not possible to change your phone's IMEI.
  - **the senders, recipients, time-stamps and subjects of emails, and whether they include attachments**. This information cannot be erased, as servers need to know who to send the emails and its attachments. However, some of it can be changed or obscured.
  - **properties of an image file**, i.e. information about the location in which a picture was taken, its size and the equipment used to produce the image (brand of camera and lens, software used to edit it) Some of this information can be erased using image processing software.
  - **properties of a document**, i.e. information about the author, the date in which a document was created or modified. Some of this information can be erased by changing the personal privacy settings of word or spreadsheets processors, or using a metadata stripping software such as the Metadata Anonymization Toolkit.[9]

Metadata is often overlooked because it is not something we ourselves create or may even be aware of. However, we should keep in mind its existence and take appropriate steps to understand its scope and the possible ramifications when considering different elements of our information ecosystem.

[9] See https://mat.boum.org

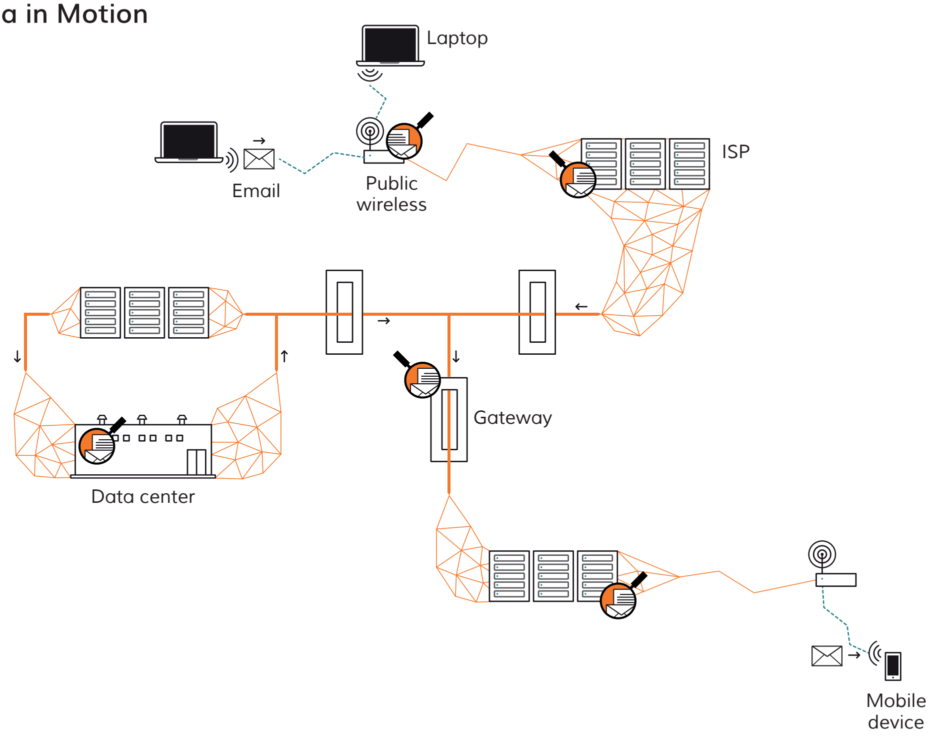
Understanding information in motion through digital channels

The above attributes of digital forms of information play an important role when we think of our information in motion through digital channels, since information can be so readily duplicated and stored. Information is in motion through digital channels when we:

- communicate using our devices; call via mobile phone, send emails, make calls using voice-over-IP, video chats, instant messaging or send text messages.
- transfer data; upload videos to the web, access a web page on our computer, back up our documents to a server located somewhere else, post an update on social media.

Information travelling through digital channels is almost always moving through physical space, e.g. a status update starting at your mobile phone will make its way to the social media website, which is physically stored on servers in a particular location, perhaps on the other side of the world. It may pass through a number of different countries along the way. In order for us to contemplate the ways we can ensure the safety of our information in motion, it helps to consider its origin, destination and the path it takes along the way.

Data in Motion



While we may know where our information originates (e.g. we type an email on our laptop), we need to pay attention to where it will end up (e.g. our colleague's inbox via their mail provider), as well as all the stops along the way, including:

- internet service provider(s)
- the telecom companies which operate internet infrastructure and transfer our data
- State entities who carry out active capturing and surveillance of data and metadata as it is transferred through the internet
- any other entity that has control over these stops and may or may not be interested in capturing the data
- other third parties like advertising companies who may gather data about our online activities.

The process of information moving digitally between spaces is relatively straightforward. Taking the time to learn or review the basics of how internet and mobile communication work helps us clarify this process. Doing so can reduce our anxiety or unfounded fears which may arise from misinformation, myths and mysteries associated with digital technology and electronic surveillance.

Consider also including the type of encryption (if any) that is used to protect the data. Encryption is a technical means of reducing the number of people who can access certain information. It is ocasionally provided by service providers (for example, banking websites or certain communication applications[10]), although often we must learn to encrypt our information or communications using particular software in order to be more certain that it won't be accessed.

Contemplating the above is also important as it may suggest additions to our actor map. We may discover we need to investigate whether there is any relationship between these actors and our allies or opponents. Having reflected on this, you may want to return to your actor map and include actors such as:

- your internet or website service provider(s)
- your telephone service providers
- providers of your email and social networking services
- any relevant entities (e.g. government agencies) who may have a relationship to the above.

These additions create a clearer picture of what exists in our information ecosystem, as well as listing any additional actors who may be involved in our work as a consequence of how our information is handled. This knowledge will equip us to protect our information more effectively. This may be through implementing policies about who can access which information, or using software which protects our information, such as for securely deleting data from our devices or encrypting our chats and emails.

In the next segment we will undertake an exercise to map our information 'at rest' and our information 'in motion'. This will help us identify the gaps in our information management practices as well as ways of bridging those gaps.

Mapping your information ecosystem

Considering all of the above, it is a useful exercise to create and maintain a map of your information, or that of your organisation, which categorises your documents and the information related to your work. This will help you to understand the current state of your sensitive information and who may have access to it, with a view to taking measures to protect it. This may include policies for who can access what data, as well as technical methods such as encryption.

This 'information map' can take the form of a text document or spreadsheet which can be regularly updated. In the following exercise, we will walk through the steps involved in creating such a document, and provide an example template which could be useful.

When creating an information map, it is useful to consider the following questions:

What information is it?

An organising principle here is to group similar types of information together. For instance, you can decide that all financial documents belong in the same category, whereas not all emails belong together. Grouping the 'what' according to type of information largely depends on the way you and your organisation work. Include software that you use here too, as the software itself can be thought of as a bundle of information, and some software can be considered sensitive.

As mentioned previously, one type of information we often don't consider with regard to digital files and communications, is meta-data. Especially with regard to information 'in motion', it is a good idea to include the meta-data of certain documents and communications (such as pictures and email files) and consider whether it needs to be removed or distorted to protect your privacy.[11]

[10] For more information on how to protect your communications, see Security in a Box https://securityinabox.org/en/guide/secure-communication

[11] For more on how to remove metadata from files, see https://securityinabox.org/en/lgbti-mena/remove-metadata and for how to remain anonymous online see https://securityinabox.org/en/guide/anonymity-and-circumvention

Where does it reside? What are the physical places or entities where your information assets are kept? These may include: file servers in the office, web servers at service providers, email servers, laptops/computers, external hard-drives, USB drives, SD cards and mobile phones.

Who has access to it? Consider the situation here as it currently is, rather than the aspirational situation. For example, in case of a person's folder of reports on an office computer, the people who have access to it may include: the person themself, any IT admin staff in charge of the server, the person's confidant, etc.

How sensitive is it? There are many ways to classify the sensitivity of a document. It is a good idea to establish an explicit categorisation for sensitive information with clear instructions on how it is to be protected. The purpose here is for you to have a scale that is consistently applied to your information which will help identify the data which is most likely to be under threat and the means by which it should be protected.

Below is an example of a three-tiered scale:

- **Secret:** only specific persons should have access to this information. There is a clear chain of responsibility for this type of information (e.g. patient files in a clinic)
- **Confidential:** this type of information is not for public consumption, but there is no specific need to preclude staff members of the organisation from access to these.
- **Public:** this type of information does not pose any risk of exposure to public. General policies however still involve their integrity and safekeeping.

It's worth noting that, in the life-cycle of a project, the sensitivity of the data involved may change. For example, if we are investigating torture in order to later make a public report about it, many of the details involved will initially be secret or confidential. Later in the project, once the data is gathered, that which must remain confidential will be separated from that which must be made public as part of the report.

Considering our information in light of these questions, we can create a document which represents a map of our information as it currently is. However, as noted above, it's important to remember that this is a live document and should be regularly updated.

2.4 Exercise

Information ecosystem

Purpose & Output The purpose of this exercise is to take an inventory of the most important information assets you manage, in order to create policies for its safekeeping later on.

Input & Materials It may be helpful to reproduce the example table below, either by printing it or drawing it on a flip-chart or other materials.

Format & Steps

Brainstorming and documentation
To begin the exercise – especially in a group – it may be useful to use a spreadsheet, or a large sheet and sticky notes, or some other means which allow you to brainstorm easily and group things together.
Brainstorm and make a list of all of the data you manage. If you're not sure where to begin, consider:

- data related to each of your human rights activities
- personal data and files, especially if stored on your work computer
- browsing activities online, especially of sensitive data
- emails, text messages and other communication related to your human rights activities.

Imagine a spreadsheet that has several columns enumerating categories as described below. Your task is to fill the rows with information.

Start with your information at rest, and for each type of information, elaborate on the following

- what information is it?
- where does it reside?
- who has access to it?

Format & Steps

- how sensitive is it?
  - secret
  - confidential
  - public
- how important is it to keep it?
- who has access to it?
- how should it be protected?
- how long should it be kept before destroyed?

Characterise and qualify the information you have mapped out. You can repeat the same process and expand the spreadsheet with additional entries for your information in motion; e.g. data being transferred (physically, electronically), communications over the internet or telecommunications networks.
The questions and example in Table 2 below may help you with this.

Remarks & Tips

This process is iterative. Once you have done the first round, you may detect patterns and groupings. For instance, you may decide that since all financial information (regardless of type) has similar sensitivities and longevity, you can group them and think of them as a financial information category.
Conversely, you might find yourself needing to expand a row into several rows. For instance, a row containing 'email' needs to be expanded to several rows to account for a subset of emails – and their safe-keeping – which is sensitive.
This should be a live document and will change according to shifts and developments in your situation. So you will benefit from regularly updating this document to account for any of these changes.

Table 1.

Information at rest				
What (examples)	Attributes			
	Where does it reside?	Who can/does access it?	How sensitive is it?	How should it be protected?
Financial documents in electronic form	Secure shared folder – file server	Executive team	Secret	Saved in hidden encrypted partition. Backed up daily to encrypted hard-drive
Program reports for the censorship campaign	Documents folder – file server	Team members, program director	Confidential	Saved in encrypted partition
Adobe InDesign for the web developer	Web content manager's laptop	Web content manager	Confidential	Licensed, password-protected

Table 2.

Information in motion					
What (examples)	Attributes				
	What method of transfer are you using?	Who has (or wants) access to it?	What physical or virtual routes does it take (origin, path, destination)?	How sensitive is it?	How should it be protected?
General emails among team members	Email (Gmail)	Team members, email provider	**Origin:** staff computers **Path:** internet (via Google servers **Destination:** staff computers	Confidential	GPG encryption
Check-ins during missions	Text messages (SMS)	Team members, telecom company	**Origin:** mobile phone **Path:** mobile network **Destination:** mobile phone	Secret	Code words

At this point you will have your initial document describing the your/your organisation's information ecosystem, which, along with the map of actors, will be invaluable as you begin the process of understanding your strength and resilience, as well as areas where you may be weak or vulnerable.

You can then begin to chart a path from identified security indicators, to specific threat scenarios, to designing strategies, plans, tools and tactics which can help you avoid these types of scenarios, or minimise their effect.

By now, we have:

- mapped out who our allies and opponents are, and the neutral parties who may become allies or opponents depending on the situation
- listed some of the relationships we, our allies, and opponents have
- created our own information ecosystem document which helps us understand and prioritise our information as it rests somewhere, or while it is travelling through various channels.

In the next Chapter we will shift our analysis to the indicators we encounter in the course of our work which may alert us to potential threats and how to systematise our knowledge of them in order to take action.

5

Security Indicators

Through carrying out regular situational analysis, mapping our vision and the actors operating with and against us and understanding our information and its role, we should now have a broader understanding of our context.

From here, we can begin to drill down into concrete security indicators: the elements we observe in our context which may indicate the threats we face or a change in our security situation, such as the emergence of new threats to our work. In this Chapter we will explore ways of looking for these in our daily life, our devices and our surroundings which may alert us to an impending danger to ourselves or to friends, colleagues and people we work with or our organisation, as well as how and where to look for these signs.

A security indicator is anything out of the ordinary that we notice which may have an impact on our security. Security indicators can include concrete incidents such as receiving declared threats, attacks against partner organisations, or suspicious behaviour of persons we may notice; however, they also include more subtle developments such as changes in the behaviour of our devices, or our health and well-being. What these have in common is that they may indicate a change in our security situation We can identify security indicators at various different moments in our daily life and work. Examples of these may include:

- receiving a letter from the authorities about an impending search of the office
- someone taking your picture without your permission, or noticing someone photographing your organisation's premises unauthorised
- not being able to concentrate and forgetting to lock the door to the office
- many unexpected pop-up windows opening when browsing the internet
- feeling exhausted even after a good night's sleep.

Like many of the previous steps, observing security indicators and utilising them as a basis for taking action to avoid harm is not necessarily new to us. In day-to-day life, people will often do this informally: for example, a series of muggings taking place in a particular neighbourhood at night will probably, when observed by others, lead to many avoiding that area or taking precautions when passing through it.

Due to the increased threat human rights defenders face as a result of their work, it often pays to just be more organised about this process. It's important to develop the habit of noting, recording, sharing and analysing security indicators with colleagues and allies regularly. This practice helps in several ways.

1. It enables us to corroborate our observations with others and understand whether our perceived notion of danger is shared and warrants action.
2. It creates a catalogue of such items, which we can later use to understand patterns of threats.
3. It alerts our allies to a situation which may plausibly impact their own security.

Identifying security indicators

We already have an instinct (our intuition) for noting peculiarities that may affect our well-being in daily life, such as somebody following us, an unknown vehicle parked outside our office or finding ourselves in a neighbourhood where we don't feel safe. Remember that these instincts are valuable, but are not absolutely accurate and may let us down on occasion.

In this regard, security indicators are more easily noticed once we have gone through a process of explicitly establishing a base-line: that is analysing and getting to know our socio-political environment, our daily life (including our homes, offices, vehicles and other surroundings), our devices and indeed our state of physical health and emotional well-being. Once we establish 'normality' in this regard, it is easier to notice anything which is 'abnormal'.

It's good to establish certain practices with which we can regularly identify and share potential security incidents. Below, we explore some good practices which you should engage with regularly in order to identify indicators and share and analyse them more effectively.

Monitoring our socio-political environment for changes in security

Observing broad trends and particular developments in the political, economic, social, technological, legal and environmental situation in which we operate, as in situational monitoring and analysis (see Chapter 2 ealier in this Section), can help identify certain security indicators. There are a number of activities you can take advantage of in order to achieve this, such as:

Talking to trusted friends, colleagues, and fellow organisations

It's a good idea to regularly check in with colleagues, friends or peers who are engaged in the same or similar activities to see if they have noticed or experienced anything out of the ordinary. This may help you to identify patterns or be on the lookout for similar indicators.

Following and documenting news

Some indicators can be drawn from sources in the media, where you can learn about changes to the interests or resources available to your allies or opponents (as you identified in your actor map), or attacks against fellow human rights defenders, which may be important indicators to note. It may be useful to regularly analyse major news events with your friends or colleagues, informally or during established meetings, in order to identify trends which may indicate a change in the security situation of your work.

Meeting experts

If you are embarking on an activity or beginning to work on an issue or in an area which is new to you, it may be useful to meet with an experienced and trusted person who can give you information regarding the security considerations of such work.

Indicators in daily activities

In day-to-day life, there are many opportunities to check and scan for things which may indicate a change in your security situation. As mentioned above, some of this is instinctive. However, as intuition can sometimes be misleading and as tiredness or stress can negatively impact upon awareness, it may be useful to consider some of the tactics outlines in the exercise below.

Note: This list is provided as a set of examples and is not exhaustive. Consider taking the time to sit with your trusted colleagues and friends to carry out or discuss the activity below.

2.5a Exercise

Security indicators in our daily life

Purpose & Output

The purpose of this exercise is to help us get an overview of our daily routines and other activities, through visualising it and noting the points at which we can check for indications of a change in our security situation.
We can use this overview of our routines to make a check-list of moments in the day where we can establish a base-line and subsequently check for potential security incidents.

Input & Materials

Use whatever drawing materials you would ordinarily use, and either a notebook, electronic document, whiteboard, etc. for creating your check-list.

Format & Steps

Visualisation: Drawing, writing
In this exercise, we suggest that you use drawing as a way of visualising your routines. Although drawing may seem strange at first, it is a useful way to externalise your routines to get a different perspective on activities you may normally not consider from the perspective of security.
Draw a typical working day, or a day during which you are carrying out an activity you consider dangerous.

Do not worry about making it too visually accurate or artistic: just enough for you to understand it yourself. Simply begin with where you are when you wake up in the morning and consider things like:

- Where you are when you have breakfast, if you have breakfast?
- If you work outside of home, how do you get there? In what vehicle, with whom, and via which areas?
- When you go to work, what devices do you bring with you? What other things do you bring (keys, wallet...)?
- Where do you work, and who else is there? How do you work and what devices do you use for that?
- If you eat lunch or dinner during work, include this. How long do you give yourself and where do you eat?
- What time do you stop working? If you work away from home, how do you get home? What route do you take?
- What do you do before you sleep? What time do you normally sleep?
- Where do you regularly spend time apart from work and home?

Once you have a picture of your day, try to look for moments where you may want to stop and establish a ‘baseline’, i.e. what a normal day looks like in order to later check for signs that anything unusual is happening in your physical surroundings. Some suggestions might include:

- The vehicle in which you travel: are there any signs of tampering (wheels, brakes, steering, ...)?
- The route you take to work: are any of these areas dangerous? Is it worth checking whether you are being followed?

Format & Steps

- Your office or workspace: is everything in its place when you arrive, and before you leave? Are the doors and windows locked?
- The space immediately around your home or office: is there anyone or anything (for example, strangers, police or vehicles) out of the ordinary here?

Note down the moments when you will check for signs of danger in your physical surroundings, and consider sharing them with trusted friends, neighbours and colleagues. If you consider yourself at high risk, you might include the daily routines of your family members or other close persons.
Create a check list from the results: what will you check, and when?

Remarks & Tips

Going through this process is meant to help identify both instances when we carry out an action or take a precaution based on our own sense of security, as well as to notice moments when we may feel a need to pay more attention or take precautions.
If you carry out many diverse activities in your human rights work, try to repeat this exercise for the different ways in which you work.

The purpose of sharing this with a trusted friend or colleague is to make ensure we double-check and confirm our observations and/or cover potential areas we may have overlooked.

Important: Monitoring indicators during dangerous activities

During more dangerous activities, such as a protest or resistance action, or a monitoring and documentation mission, we have to be particularly aware of security indicators, especially given that the situation around us may change quickly. Consider carrying out the activity above for these particular activities and make a note of any different moments in which you should be sure to check for possible signs of danger in your physical surroundings. Make your own check list!

Digital security indicators

We may be somewhat accustomed to looking for security indicators in our socio-political environment or the physical realm or in our daily life. However, threats which arise in the digital realm are increasingly relevant to human rights defenders: censorship of websites, confiscations of computers and other devices and electronic surveillance are commonly used to gather information, intimidate and/or attack human rights defenders.

It may take a little more time and skill to notice security indicators in the digital realm. When it comes to digital security, we have not yet developed an evolutionary instinct for identifying or reacting to threats, dangers or even noticing signs that may indicate a threat to our information. Furthermore, due to varying and often limited access to technology, we may not have much knowledge about digital devices and the concept of digital insecurities itself can seem overwhelming. It is possible to develop this knowledge and comfort with digital technologies, but we often have to start from the beginning and learn what signs to look for in our devices and systems which may alert us to an irregularity. Irregularities include any interruption of normal function of our devices and may include problems such as:

- sluggish start, operation or shut down of your device
- erratic cursor movements on the screen
- unusual emails or text message from known contacts
- unknown persons contacting you with information they shouldn't have
- phishing attempts: emails claiming to be from known contacts, your email provider, social networks or others which attempt to convince you to download an attachment or click on a link in order to obtain your login details or infect your computer
- unread emails appearing as 'read'
- emails or other notifications about failed login-attempts into your accounts such as your email, social networking accounts etc.
- the battery on your phone or laptop running out unusually fast.

Identifying digital security indicators

There are some useful practices which, if carried out regularly, can help you to establish a baseline (i.e. 'normal' functioning) and later identify indicators which might otherwise go unnoticed. You can monitor the outcome of the activities below and with documentation and review, identify any changes and see if they amount to a security indicator corresponding to a possible threat.

- Scan devices with an anti-malware program to see if you have malware or spyware.
- Check your firewall to see what information leaves and enters your device.
- Check what processes and programs are running on your computer and your mobile phone, to see if some are unauthorised.
- Use two-step authentication for your online services where possible, so you can detect whether others have attempted to impersonate you.
- Make physical marks (such as with UV marker) or use tamper-tape on your devices and take pictures of them to help you verify if they have been tampered with.[12]

For more in-depth information on searching for security indicators, see **Appendix B.**

Indicators in our health and well-being

Another space in which to explore security indicators is within ourselves, our physical experience and our feelings. Our emotional situation might hint of external threats as much as to a condition within ourselves which might prove problematic to our overall security situation. Someone who is exhausted, burnt out or depressed is unlikely to be as secure or effective as they would be if they were healthier or better rested. Being sensitive towards ourselves and handling our emotional and physical vulnerabilities with care may contribute to our security as much as it might prove a source of inspiration and power.

Some common security indicators we might identify in this regard include:

- changes in sleeping patterns
- always feeling tired
- finding it very difficult to work in a motivated and focused way
- sudden mood swings
- becoming irritated or angered by small things
- feeling sad or down much of the time
- being unable to stop thinking about bad things that you have experienced or witnessed
- changes in your appetite or eating patterns
- increases in the amounts of alcohol, drugs or medicines that you consume
- thoughts about ending your life.

[12] For more on physical protection of devices, see Security in a Box: "Protect your data from physical threats" https://securityinabox.org/en/guide/physical

Many people are used to noticing these indicators in the course of their daily life and taking action to rectify the situation. However, as activists we sometimes continue to push ourselves and risk causing lasting damage. Sometimes, we can get so caught up in our work that we don't even realise or pay attention to what we are feeling in our own minds and bodies. Therefore, as with everything we have covered until now, it is a good idea to try to be methodological about taking care of our physical, emotional and psychological selves. One such way of doing this is by making a stress table.

2.5b Exercise

The stress table

Purpose & Output

This exercise can help you to identify your limits concerning different kinds of stress, how to recognise these limits and measures to counter stress. Take some time, ideally when you are not under stress and try to create your own stress table.

Input & Materials

For this exercise we differentiate between three levels of stress, like a traffic light:

Green = bearable, motivating stress. This kind of stress might keep us creative, but we may become tired more easily, need more breaks and know that we don't want to feel it for a long period of time.

Yellow = unpleasant stress. With this level of stress, we may feel tired and at the same time alert. We may manifest physical signs of stress (which vary from person to person). We will usually have a strong desire to change the situation which is causing this sensation.

Red = unbearable, profound and lasting stress. This kind of stress affects different spheres of our lives including our relationships at work, with our friends and family as well as

Input & Materials

our personal relationships. This level of stress also reduces the pleasure and relaxation we take from recreational activities, and we feel anxious and/or miserable. Our bodies show clear physical reactions, and we may feel close to collapse, and resort to unhealthy measures to stay alert, such as stimulants.

Format & Steps

Step 1: Basing yourself in the example below, draw up an initial stress table and reflect on it with somebody you trust.

Step 2: Decide on a regular schedule, when you want to review your stress status, and try to carry out these reviews accordingly.

Step 3: If you frequently experience high stress levels over a period of time, review your stress table to determine if it is still adequate.

Remarks & Tips

Checking this stress table could be one step in your personal security guidelines and should be done regularly. Be sure to check if your definitions for the different levels are still accurate, or if you have simply become accustomed to higher stress levels!

	Indicators (How do you recognise that you are at this stress level? What makes this phase qualitatively different from the previous level?)	**What can you do to reduce the level of stress, or increase your ability to cope?**	**Resources needed**
Green			
Yellow			
Red			

Bear in mind that emotional dangers are sometimes subtle and can creep up on us. They increase slowly over time and we may fail to notice how much has changed. Some strategies for regularly scanning for indicators of emotional danger include:

- paying attention when friends and family comment on your mood, appearance or interpersonal behaviour
- actively seeking out feedback from trusted friends and colleagues who care about you enough to be truthful with you
- keeping a private diary of your thoughts and feelings from day to day
- paying attention to ways in which your stress level might be making you less aware of security indicators (physical, informational, or emotional) in your environment;
- if necessary, seeking advice and support from a mental health professional.

Sharing and analysing security indicators

It's very important that we share and analyse security indicators with trusted friends or colleagues in order to establish whether they are worth taking action. It may well be the case that one or more people involved in your activities have notices similar signs, having observed the same or similar indicators.

If you work for an organisation or group which has regular meetings, including security indicators as a regular agenda item for discussion is one way of ensuring that they are analysed. When sharing incidents and noting security indicators is seen as a valuable activity, it naturally happens more frequently and informally too.

Steps to follow in the analysis of security indicators[13]

In the case of particularly important security indicators, such as concrete incidents, it may be useful to ask the following questions as a basis for analysis.

1. **What happened?**
2. **When did it happen?**
3. **Where did it happen?**
4. **Who was affected?**
5. **Was gender-based violence (GBV) involved?** This is especially important in the case of concrete incidents involving third parties. Consider physical and psychological factors.
6. **In the case of aggressions–who was responsible?**
7. **Why do we feel this happened?** Try to avoid being accusatory here but rather establish the facts of the incident.
8. **What was its origin?** Was this related to common delinquency, environmental factors or our work and activism?

[13] Based on Peace Brigades International Mexico Project (MEP, 2014) Programa de Asesorías en Seguridad y Protección para Personas Defensoras de Derechos Humanos, p.82

As security incidents are generally 'sensitive' information, it's good to discuss and analyse them in a digitally, emotionally and physically 'safe' space. Keep the following factors in mind:

- If you are sharing indicators remotely (e.g. during field work), consider the channel you use to communicate them. To allay fears, it may help to speak to someone over the phone, but keep in mind that this may not be secure. You may want to use a more digitally secure channel, such as encrypted text messages or emails.
- Noting and sharing indicators among your group is a service to yourself and your peers and should be treated as such. Indicators, even when they are internal, are not necessarily anyone's 'fault'. Above all, they should be considered in light of what they may mean for everyone's security. Sharing an indicator is a moment for appreciation, not a moment for shaming.
- When sharing security indicators that relate to a person's behaviour, it is helpful to include positive security indicators (when a person took an appropriate security precaution, or when the political situation changes in our favour) as well as critical indicators (when an action or inaction was noted). Sharing these in a positive, non-judgemental setting is crucial to you and your peers and colleagues' ability to benefit from the openness of the discussion, and look for collective solutions, instead of placing blame and marginalising people.

Maintaining a register of security indicators

Whether working as an individual, a group of friends or a formal organisation, it is important to create a space where you can record security indicators in as much detail as possible, in order to later share and analyse them. This may take the form of a document or spreadsheet which should be periodically analysed (weekly or monthly) so that any trends in the indicators can be noted.

In a group or organisation, it's useful to designate someone to maintain the registry of indicators and store them in a secure manner. By any standard, a registry of security indicators should be considered highly sensitive information and only shared with trusted partners. Of course, in some high-risk actions such as a protest, the only space you can use to record incidents may be your own mind. In such cases, it's best to find a friend or colleague with whom you can share details of the incident as soon as possible.

Example: Register of security indicators

When? ....

....

Where? ....

....

Who? ....

....

What happened? ....

....

Analysis (GVB? Responsible? Why?: Origin?) ....

....

....

....

Note: Some people may not feel comfortable having their personal or emotional security indicators recorded in such a document. As a rule of thumb, it's always best to ask if people are comfortable with this and respect the wishes of those who are not. In these cases, it is important that they nevertheless have a safe and comfortable social or professional space to share these feelings in as much confidentiality as is appropriate.

6

Identifying and Analysing Threats

In this Chapter, we will build on our analysis to identify concrete threats to our well-being. Threats, for the purposes of this exercise, refer to any potential event which would cause harm to ourselves or our work.

The process of identifying and analysing threats is not new to us. In daily life, this is something many of us do naturally and almost without conscious effort. Crossing a busy street is fraught with possible dangers but those of us living in urban areas are usually able to do so safely, employing our ability to identify threats, such as an approaching bus or a motorist in a speeding car, and taking measures to minimise their ability to harm us.

In order to do this, we rely on our prior knowledge as well as processing new information. We take into account environmental factors (is the road surface wet due to rain?), social norms (crossing anywhere on the road in some cultures versus only using pedestrian crossings in others), and who possible allies and opponents are (a police officer, the driver of the bus). Some of our prior experience allows us to cross streets in unfamiliar places, but we may also need more information in a new situation, such as the norms and laws in another city. For example, cycling commuters and bicycle lanes in some European cities can be a surprising danger for someone who is used to interacting only with motor-vehicles when crossing streets. Similarly, in our work and activism, we are usually able to identify some of the threats we face and take steps to reduce or prevent them. However, with the context changing around us, we may encounter threats we do not notice or know about. Our preparations will help us have a more comprehensive picture of the threats we might be facing.

Through following the exercises in the previous Chapters, you may have accumulated a body of knowledge about your situation, including your vision, the environment in which you operate, your allies and opponents and their respective resources and limitations, what comprises your information assets and identifying security indicators which help you to remain aware of your security situation.

This information should leave us well prepared to identify threats to ourselves, our group or organisation. We can substantiate the threats we perceive by gauging the resources and abilities of our opponents, identify previously unnoticed threats to our information ecosystem and using the indicators in our preparations to prevent, defend against, respond to, or resolve such eventualities.

Note: It is, however, important to keep in mind that not all the threats to our well-being and security are political or related to our work. We should also be mindful of threats which may arise from delinquency, petty crime, gender-based violence, environmental hazards, etc. Although these do not necessarily represent a political response to our work, they can be among the most important threats to human rights defenders.

In this Chapter we can start with what we feel to be existing threats against us and scrutinise them. We will also use the previous steps in this Section as a starting point for identifying the underlying potential threats. Using the previous findings, we will then be in a position to evaluate these threats based on what we consider to be the **likelihood** that they would happen, and the extent of the **impact** or damage if or when they do.

Our response to them is also categorised similarly around the above two concepts and can be thought of as a combination of the **prevention** and **response tactics** we will employ. In the subsequent Chapters, we will come up with preparations and actions to minimise the likelihood of these threats, as well as steps and actions we will take to reduce the damage of threats that are carried out.

2.6a Exercise

Threat brainstorm

Purpose & Output

This exercise is a first attempt at identifying the threats to yourself, your group or organisation and your work in defence of human rights. This initial list of threats can then be refined so as to focus in more depth on the threats which are most likely or potentially most harmful.

Input & Materials

Inputs: this exercise will be easier if you start with:

- your analysis of the ongoing political, economic, social and technological trends in your context
- a list of the activities or types of work you carry out in order to achieve your objectives
- your actor map, particularly the opponents
- a list of security indicators you have observed in your previous work.

Suggested materials:

- **If alone:** a sheet of paper or some other materials for writing.
- **If in a group:** a large sheet or flip-chart and writing material.

Format & Steps

Consider and write down all the potential threats to yourself, your organisation and your work. It may be helpful to categorise them beginning from each of your activities or areas of work. Remember: a threat is any potential event which could cause harm to ourselves or our work. Don't forget to consider potential threats to your information security and threats to your well-being, political or otherwise.

Create a list of these threats. If you find it difficult, consider your opponents and the ways in which they have acted against other human rights defenders in the past. Analyse your security indicators and consider whether they represent a concrete threat.

Format & Steps

Observe any patterns that emerge in the threats you identified: do they relate primarily to certain activities of yours, or originate from certain opponents? This will be useful when it comes to security planning (i.e. by planning particularly for certain activities, or dedicated plans for engagement with some actors).
Keep this list for analysis in the following exercises.

Remarks & Tips

If the list is somewhat long, it may be overwhelming to consider these potential threats. It may also be a challenging exercise as we may not know how realistic we are being.
It's important to remember that political threats always originate from a certain actor or set of actors who see their interests potentially threatened by you and your work. In a sense, threats are a sign that your work is effective and that your opponents fear your work. While it may be a moment which inspires fear, clearly recognising the threats you face should also be a moment of empowerment. Acknowledging these threats and the likelihood of their occurrence allows you to better plan for and potentially mitigate the damage caused to you or you work, should one of them occur.

Perceiving threats

As previously mentioned, our perception of threats is sometimes challenged for a number of reasons: perhaps the information available is limited; perhaps fear, stress or previous traumatic experiences have an impact on our perception and can lead us to experience unfounded fears ('paranoia') or to fail to recognise threats. Both of these occurrences are quite natural, although they are not desirable. Therefore, it's a good idea to be aware of this and find mechanisms for checking our perception – either through further research or through consultation with people we trust.

In the next exercise, we pose some questions which may help you to think critically about your perception of threats and devise tactics for making your perception more accurate.

2.6b Exercise

Reflection on perceiving threats

Purpose & Output

Improving the recognition and analysis of threats in order to respond adequately.
You will learn to recognise your own blind spots and missing processes for identifying threats as well as creating processes to fill these gaps.

Input & Materials

Use the list of threats from the threat brainstorm (Exercise 2.6a) for this exercise.

Format & Steps

Individual reflection or group discussion

Ask yourself or the group the following questions:

1. Were there any threats which you discovered or which were mentioned by others, which you wouldn't have been aware of previously?
2. If you did the exercise in a group, was anyone else surprised by the threats you mentioned? Why?
3. How long do you think the threats you identified existed before you became aware of them?
4. How might you have become aware of them sooner?
5. How do you communicate in your group, with your colleagues about them?
6. What makes them feel more or less serious?
7. Can you identify any threats that feel more serious than they might actually be?
8. If you are working with a group: what are the differences in your answers to the above? What makes you think of the same threat in different ways?

Remarks & Tips It can be overwhelming listing all the threats you face. Be sure not to rush this exercise and to allow space for people to express their feelings as they go. If you find this exercise useful, consider making it a regular (weekly or monthly) exercise.

Prioritising threats: analysing risk

As we begin the process of identifying all the threats or obstacles which may affect us or our work, it is important to avoid becoming overwhelmed. If we brainstorm threats, we may indeed come up with a long list and not know where to start; furthermore, this may be aggravated by unfounded or exaggerated fears. This is why, as in the previous steps, analysing each threat can be helpful. Threats can be viewed and categorised in light of the following:

- the likelihood that the threat will take place
- the impact if and when it does.

Likelihood and impact are concepts which help us determine risk: the higher the likelihood or impact of a threat, the higher the risk. If a threat is less likely or would have a lower impact, the risk is lower.

Of course, in undertaking such an exercise, we must be aware that we are relying on our own perception. As we explored in previous Chapters, our perception can face a number of challenges when we are tired or stressed, or when we talk about threats outside our area of expertise (for example, threats to digital information, for HRDs who are less comfortable with technology). It is important to keep this in mind, comparing our perceptions to the perceptions of others, and carrying out research where necessary to verify them.

Likelihood

To gauge the likelihood of the occurrence of a threat, we can make use several sources of information, including: the actor map we created, our analysis of historical security indicators, and our allies' experiences in similar situations. This process is not expected to deliver the exact probability of a threat actually occurring, but rather to help us prioritise those threats we deem imminent. Generally, they can be grouped into the following categories.

Unlikely to happen These are threats for which there is little precedent and few favourable conditions to facilitate them. While we may choose to 'down-prioritise' these, we should keep them in mind, especially if their impact would be substantial (see below). Furthermore, it is important to record these, because as our socio-political context changes, their likelihood might also change.

Likely to happen These are threats with clear precedents and/or very favourable conditions to facilitate them. These threats are prioritised for our next steps.

Unclear, or don't know In some cases, our information and intuition may not arrive at the same answer, or there may not be enough information to comfortably categorise the potential threat into likely or unlikely. In this case, it is important to err on the side of caution:

- investigate further regarding the potential threat with the help of our allies and their experiences, trusted subject-matter experts, or deliberations within our group, until we can safely put them into one of the above categories, OR;
- move them to the 'likely' category anyway.

Impact

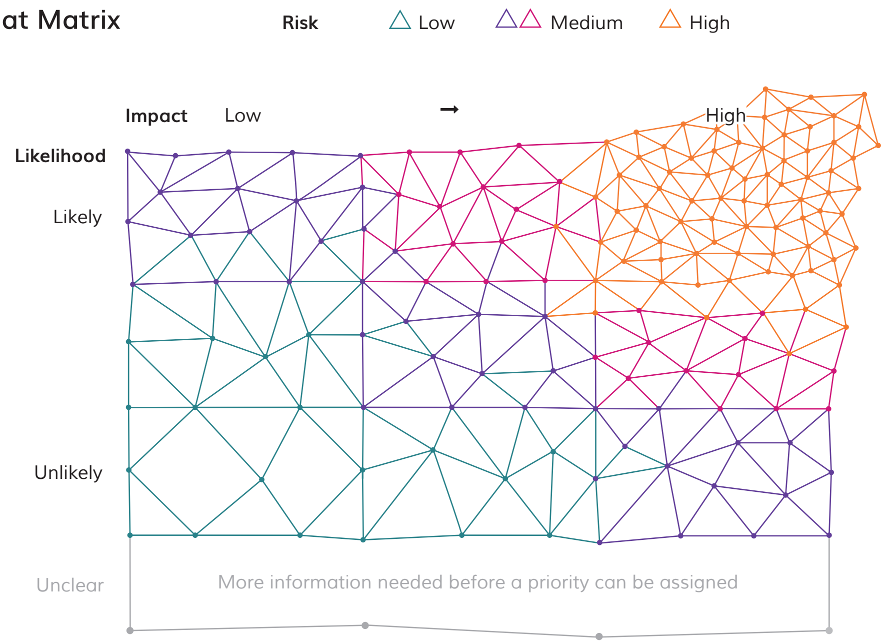
When analysing what the potential impact of a harmful event would be, it is helpful to imagine a scenario whereby the threat already took place. In this scenario, how has the threat harmed us? Examine the situation and reflect on questions like:

- How many people are affected?
- How long-lasting is the effect?
- To what extent does this hamper our normal operations?
- What other harmful situations does it enable?
- Is there an immediate danger to other people still not affected?

According to your own standards, you can consider the threats to be of low, medium, or high impact. Low-impact threats should only have limited negative impact on your ability to continue your work, whereas threats should generally be considered high impact if they would prevent you or your organisation from carrying out your activities effectively in the medium- or long-term.

It may help you to visualise the likelihood and impact of the threats you have identified by plotting them on a matrix such as in the example below, noting that generally speaking, the priority threats – those which are 'higher risk' – will trend towards the upper right corner.

Threat Matrix



By considering the threats we identified in light of their likelihood and impact, we can then move towards a deeper analysis of them, the conditions required for them to happen and their potential consequences, which will aid us in planning to react to them.

Declared threats

Consider the possibility that we are faced with an explicit declaration of an intention to hurt us, e.g. a message from an individual, group or organisation that openly expresses their intent to cause us harm. These are also often referred to as 'declared threats' and are often made to human rights defenders in the form of text messages, phone calls, emails, verbal abuse or letters. They may alternatively be implied in our opponents' public statements or through judicial harassment, proposed legislation or many other methods. Their intention is to inflict damage on our work, to punish or hurt us and discourage others in turn. Such messages constitute a special kind of security indicator because they already have an an impact (psychologically), and might well correspond to an actual threat. They deserve our attention to establish their veracity and severity.

Generally, 'declared threats' are:

Intentional they are made with a clear intent to intimidate us and discourage our work

Strategic they are part of a larger plan to prevent or hinder our work

Personal they are specific to us and our work

Fear-based they are meant to scare us so that we cease our work.[14]

It is important to keep in mind that while some threats may be real, others are intended to create new unfounded fears while no actual action to harm is planned by the individual or group who made the threat. When analysing this kind of indicator, you might find it helpful to go back to your actor-mapping and consider the resources and interests of the adversary in question.

Such threats are very 'economical', as they may achieve the same result as an attack, without the effort or possible expense of actually carrying it out. (As mentioned previously, identifying unfounded fears is an important part of developing an effective holistic security plan.) All the same, receiving such a message can itself be a very shocking experience and may inspire a lot of fear in us. It is important, as far as is possible, to create a safe space for ourselves or our group (emotionally, digitally and physically) in order to debrief, discuss, analyse and respond. For a suggestion of steps to take regarding analysing declared threats, see Appendix B.

Unfortunately, not all threats we may face are directly and explicitly noticeable. The results of our preparation in the previous Chapters are an invaluable resource for identifying, analysing and responding to threats we perceive. In this Chapter, we will employ our security indicators, our information ecosystem documents, as well as our actor and relational maps and situation analysis.

In the next exercise, we will begin with the list of threats we identified in the brainstorm, assign them a priority, and expand our understanding of their nature. It is important to also note that for many threats, our state of mind and body also plays a role in determining the probability as well as impact of any given threat.

[14] See Front Line Defenders Workbook on Security for Human rights Defenders and Protection International: New Protection Manual for Human Rights Defenders http://protection-international.org/publication-page/manuals/

2.6c Exercise

Threat inventory

Purpose & Output

This exercise will help you prioritise threats and divine the causes, ramifications, sources as well as the required resources, existing actions and possible next steps.
The output of this exercise is an inventory of your prioritised threats in some detail, which will be used in the next Chapter to help you create plans of action.

Input & Materials

- Actor and relational maps
- Information ecosystem
- Security indicators
- Impact/likelihood matrix

- Pens and paper
- Flip-chart
- Markers

Format & Steps

First, beginning with the threat brainstorm from the previous exercise, consider the threats listed in terms of their likelihood and impact. Make a selection of those you consider to be most likely and as having the strongest impact to use for the next exercise.
Again, it may be useful to separate and organise threats according to particular activities (e.g. separating those which specifically arise in the context of protests from those which relate to the day-to-day running of your office).
Start with what you consider the highest priority threat, based on the impact/likelihood matrix, and using the example template provided, elaborate (individually or in a group).

- Write down the title and summary of the threats.
- For each threat, if it is a complex threat, you may decide to divide and analyse sub-threats (for instance, an office raid and arrest may be easier to analyse if separated to include the numerous consequences each would include – potentially arrests, confiscation of devices, judicial harassment, etc.). Use the rows to expand each of the below per sub-threat.

Work through the following questions for each threat. It is possible that some threats are complex, and some of the answers require their own space. Use as many rows as necessary. If, for instance, a threat constitutes an attack on a person, as well as the information they are carrying, you may want to use one row to describe the informational aspects and another for the person in question.

- **What:** Describe what happens if the threat is carried out. Think of the impact it might have on you, your organisation, your allies. Include damages to physical space, human stress and trauma, informational compromise, etc.
- **Who:** Identify the person/organisation/entity behind the threat: Referring back to the actor map, you can focus on information regarding this specific adversary:
  - What are their capabilities?
  - What are their limitations to carrying out these threats?
  - Are there neutral parties or allies that can influence them?
  - Is there a history of such action against you or an ally?
- **Who/what:** identify the potential target of the threat; specific information being stolen, a specific person under attack (physically, emotionally, financially), material and resource under threat (confiscation or destruction of property).
- **How:** What information is needed?
  - What information is necessary for the adversary to be able to carry out the threat?
  - Where might they get this information?
- **Where:** describe the place where the potential attack might take place.
  - Does an attacker need access to the same location as you, as is often the case in a physical attack?
  - What are the characteristics of the location in question? How can we you it to keep safe? What is more dangerous about it?

Format & Steps

Elaborate on the psychological, emotional and health factors as they relate to this threat, including the effect your stress levels, tiredness, fear and other factors on the potential occurrence of this threat. Consider:

- How might your current mindset affect any planning and contingency measures being carried out?
- Does this threat take place in the context of a particular activity? What kind of mental or physical state do you find yourself in during such activities? What are some best practices which may protect you, or what might make you more vulnerable?
- What elements of your behaviour or state of mind may actually increase the probability of this happening, or its impact?

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				

Now that you have identified a list of the threats that may arise in the course of your activities, along with who may be behind them, you can make plans and prepare for two inter-related objectives:

- to reduce the likelihood of the threat ever happening
- to minimise its impact if it does come to pass.

Remember that the above list is not a static list, and revisiting the process is very important. Shifts and changes in the context invariably affect the landscape of your work. Unforeseen threats may develop, or the likelihood of certain threats may be reduced due to external factors. You can determine how often you should revisit these lists and set time aside for it.

Conclusion

In **Section II | Explore**, we have followed a series of steps in order to analyse our context, beginning with the general (e.g. political, economic, social, technological, legal and environmental factors) and moving gradually towards identifying specific threats to our security.

In the next Section, we will take steps to prepare ourselves in order to reduce the likelihood of threats occurring and their impact, examining our existing capacities and vulnerabilities relative to these threats, and from there, building security strategies, plans and tactics.

We also have to consider how we can integrate these steps into our existing routines and work in order to maintain an up-to-date analysis of our context, and build consistent organisational approaches to managing our security and well-being.