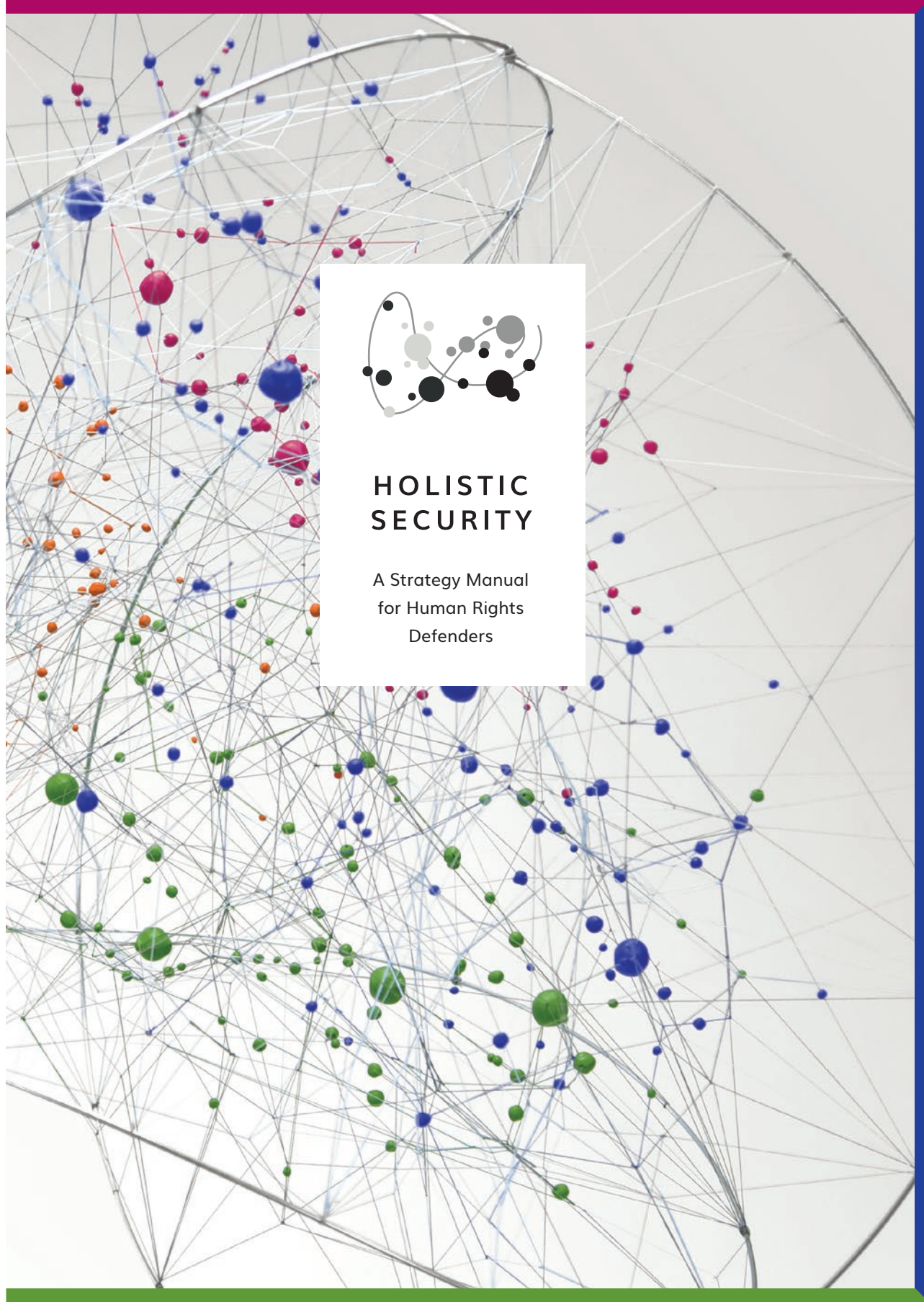


HOLISTIC SECURITY

A Strategy Manual for Human Rights Defenders

HOLISTIC SECURITY

A Strategy Manual
for Human Rights
Defenders

Published in 2016

Credits

Authors
Craig Higson Smith for Center for Victims of Torture
Daniel Ó Cluanaigh for Tactical Technology Collective
Ali G. Ravi for Front Line Defenders
Peter Steudtner for Tactical Technology Collective

Additional writing
Magdalena Freudenschuss for Tactical Technology Collective
Sandra Ljubinkovic for Tactical Technology Collective
Nora Rehmer for Protection International
Anne Rimmer for Front Line Defenders

Coordination
Project lead Daniel Ó Cluanaigh
Coordinator Hannah Smith
Art and graphic design La Loma GbR
Copy editing Johanna Whelehan

A project of
Tactical Technology Collective

In collaboration with
Center for Victims of Torture
Front Line Defenders

With special thanks to
Wojtek Bogusz, Emilie De Wolf, Jelena Djordjevic, Enrique Eguren, Andrea Figari, Ricardo Gonzalez, Stephanie Hankey, Oktavía Jonsdottir, Becky Kazansky, Tom Longley, Chris Michael, Eleanor Saitta, Bobby Soriano, Niels Ten Oever, Marek Tuszynski, Arjan van der Waal, Pablo Zavala;

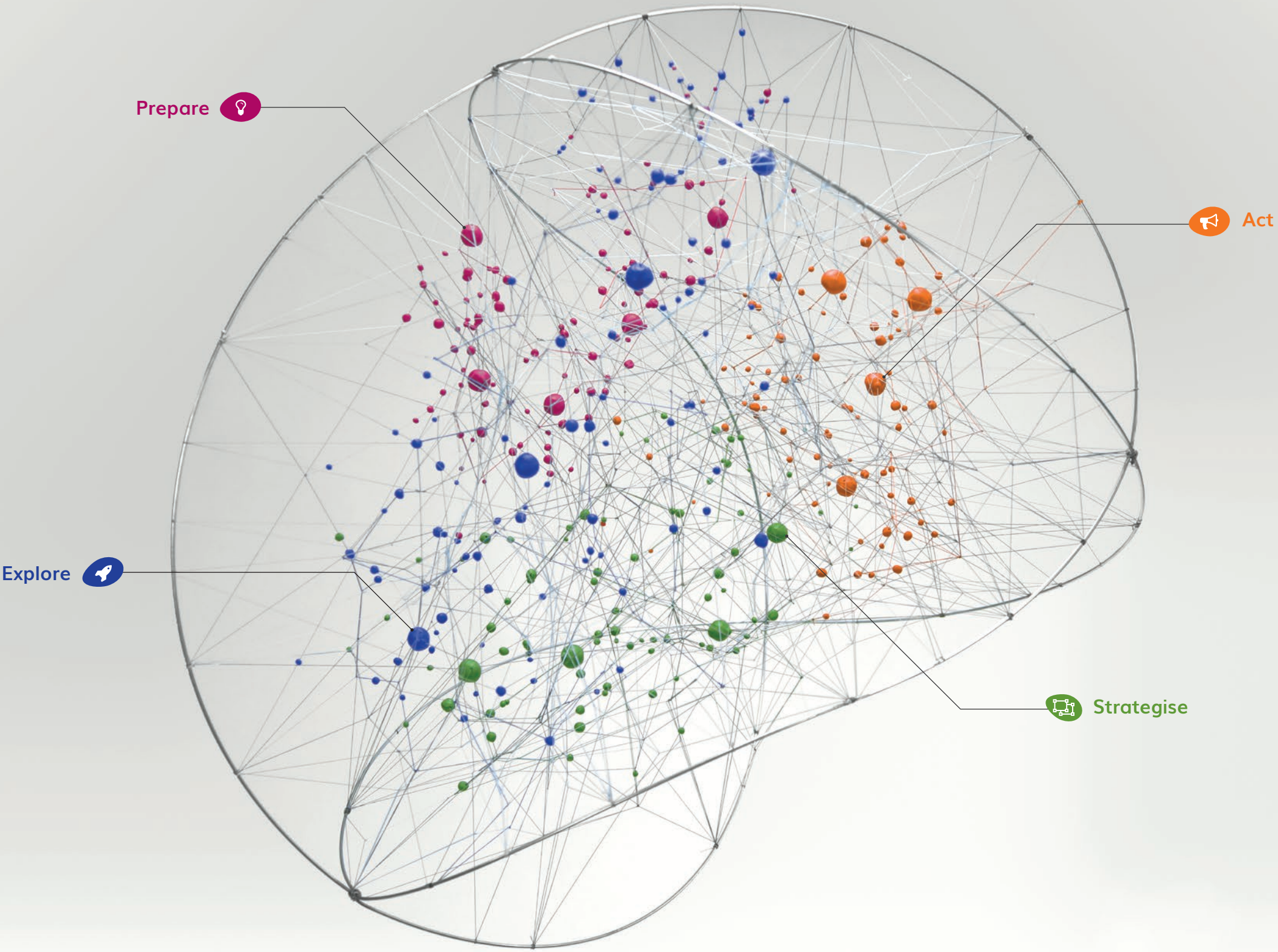
our friends and colleagues from
Article 19
Centre for Training and Networking in Nonviolent Action "Kurve Wustrow"
IREX S.A.F.E Initiative
Protection International
Tactical Technology Collective

and the community of security trainers, experts and human rights defenders with whom we have collaborated and learned throughout the process of creating this manual.

Funders
This publication has been produced with the assistance of the European Union

with additional support from Hivos.

The contents of this publication are the sole responsibility of Tactical Technology Collective and can in no way be taken to reflect the views of the European Union.


Prepare
Act
Explore
Strategise

Contents

Introduction

"Caring for myself is not an indulgence, it is self-preservation and that is an act of political warfare."

Audre Lorde

Over two decades ago, the United Nations Declaration on Human Rights Defenders[1] was adopted by the United Nations General Assembly, recognising the right of individuals and organisations to (voluntarily or professionally) strive to preserve, promote or propose human rights as they relate to themselves, their communities or their causes.

The term human rights defender (HRD) therefore refers to anyone who promotes or defends any of a vast array of rights which may include civil and political rights (such as freedom of speech or justice for survivors of abuse); transparency and anti-corruption or greater political participation; environmental rights, social justice, and cultural rights; rights related to sexual orientation and gender identity, or advocating for the recognition of new human rights. Regardless of their given profession or the human rights they promote, recognition of the work of human rights defenders under international law, as well as under the laws of numerous States, affords HRDs an additional layer of protection to carry out the work that they do.

Unfortunately, human rights defenders continue to suffer attacks at the hands of both State and non-State actors which impact upon their physical and psychological integrity, and often further affect their friends and families. Those opposed to HRDs' work seek to close down the space for free and peaceful association, communication, expression, organisation and the support of survivors of human rights violations.

For example, women human rights defenders are frequently targeted for (often sexualised forms of) violence, due to their work challenging normalised patriarchal discourses, laws and traditions. Those working on the rights of Lesbian, Gay, Bisexual, Transgender and Intersex (LGBTI) persons and other sexual orientation and gender-identity issues are often similarly targeted and marginalised by existing power structures. Environmental rights defenders, as well as anti-corruption defenders, find themselves targeted for personal, economic and societal attacks by private companies acting through State or non-State agents. In addition to all of the above, recent years have seen the development of increasingly complex electronic surveillance mechanisms which encroach upon our personal lives and into our daily activities, communications and ways of working. This factor poses a significantly greater threat for human rights defenders, who may find themselves exposed, their sources compromised or their work jeopardised as a result of their online activities.

In the vacuum created by a lack of adequate protection by the State, security and protection become key issues for human rights defenders: at home, at work and while carrying out activities to promote or defend human rights. The purpose of this guide is to help HRDs take an organised approach, building strategies to maintain their well-being and creating space for activism and resistance, whether working alone, in small groups, collectives or organisations.

About the holistic approach

This guide is the first to explicitly adopt a 'holistic' approach to security and protection strategies for human rights defenders. In short, this means that rather than looking separately at the importance of our **digital security**, **psycho-social well-being** and **organisational security** processes, it attempts to integrate them and highlight their interrelatedness.

In the past, the various aspects of human rights defenders' security have tended to be treated separately, as if they existed in isolation from one another. However, this 'compartmentalisation' of deeply interrelated aspects of our security greatly limits our ability to adopt a comprehensive approach in a number of ways, including:

- Lack of adequate awareness of the emotional and psycho-social aspects of security often blinds us to potential threats, such as the effects of long-term stress on our health. Furthermore, fostering mental and physical well-being benefits our ability to understand our security situation and take critical decisions.
- With increasing digital surveillance of activists, lack of adequate understanding of the digital technologies we use in the course of our work can also greatly limit our ability to accurately perceive the threats around us. Achieving this understanding and taking proactive decisions to protect our data

1 http://www.ohchr.org/EN/Issues/SRHRDefenders/Pages/Declaration.aspx

from unwanted access or surveillance not only means a more comprehensive approach to our overall security, but also provides us with relative certainty regarding the source of threats which can be highly secretive and difficult to perceive.

- Adopting security measures in an ad-hoc manner or based on 'tradition' or hear-say, without carrying out an analysis of our context and the threats we face, often leads to us taking decisions which give us a false sense of security. Therefore, it's vital that we regularly map out the socio-political context in which we are acting, identifying as accurately as possible the threats that we face and updating the strategies, tools and tactics we can use to defend our space and continue working in an empowered manner.

Following on from important work carried out by others in establishing the 'Integrated Security' approach, the holistic approach in this manual is founded on the understanding that 'security' is a deeply personal, subjective and gendered concept. Indeed, security takes on a special meaning when we consistently find ourselves in danger as a result of standing up for our rights and the rights of those around us. Therefore, our approach must take into account the subjective and personal nature of each journey in defence of human rights. Any attempt at a 'rational' understanding of our security situation must consider, accept and embrace our own inherent irrationality.

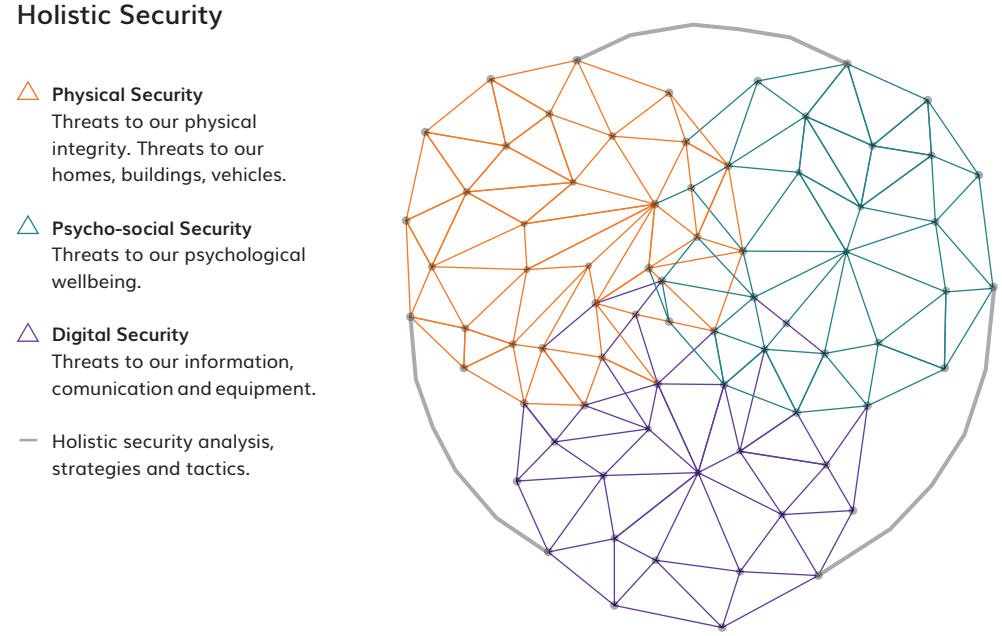
Our approach to security and protection must take into account the effects not only of physical violence, but also structural, economic, gender-based and institutional violence, harassment and marginalisation. This may be perpetrated by the State, but also by private corporations, non-State armed groups, or even our own communities and those close to us. It can deeply affect our psychological well-being, our physical health, and our relationships with friends, family and colleagues. Awareness of, and action regarding these threats is vital in order for our activism and resistance to be sustainable, and in order to facilitate our ability to identify and implement strategies for our security and protection. As such, we understand and assert self-care, all too often considered 'selfish' among activists, to be a subversive and political act of self-preservation, and one which is fundamental to effective security strategy and culture.

Our security strategies also have to be regularly updated. As the context around us changes, so do the tasks and challenges in integrating security into our work. This is particularly true in an era in which we have become increasingly dependent on digital tools and platforms for our activism: computers, mobile phones, social media, digital cameras and other technological solutions have become

indispensable to our work, but they also work against us as tools of surveillance, identification and harassment by States, armed groups, companies, communities and families.

As such, comprehensive security must not only include our bodies, emotions and mental states, but also the electronic information contained in devices in our hands, pockets, bags, homes, offices, streets and vehicles. We can not fully understand our security or well-being without taking due account of the role of the digital dimension in our personal lives and activism. This manual, therefore, explicitly integrates the need for an understanding of our technical environment and its relation to our work and our security.

Holistic Security



Prepare, Explore and Strategise

The content of this edition of the manual is divided into three Sections: **Prepare**, **Explore**, **Strategise**, while the fourth Section, **Act**, is available on-line. These steps are conceived as an evolving **cyclical** process, which should be regularly revisited as part of your existing strategic planning.

In **Prepare**, we begin by recognising that each of us already has and takes security measures: our strategies for health and well-being, our personal beliefs and sources of resilience and our instinctive responses to threat and danger. We encourage you to consider these and their effect on group dynamics which must be recognised in order to engage with security strategies in a more productive way.

In **Explore**, we follow a series of steps in order to analyse our socio-political context and come to some conclusions about the concrete threats which may arise from our work and those who oppose it.

In **Strategise**, we begin with the threats we have identified and consider how to create security strategies to deal with them, as well as develop concrete plans and agreements in order to maintain our well-being in action.

Engaging in these three steps prepares us for the fourth step: learning new tools and tactics for our security in action – **Section IV | Act**. To this end, this manual is accompanied online by short, scenario-focused guides which focus on concrete tools and tactics – from the technological to the psychological and beyond – for security in particularly high-risk activities which are common to many human rights defenders.

How to use this manual

This manual is designed to guide a process of establishing or improving security strategies for individuals, collectives or organisations. We use the term human rights defender to be as inclusive as possible and hope that the manual will be of use to people working in a variety of different capacities, from grassroots defenders and community organisers to lawyers, journalists and activists. Although it is written in a linear narrative format with a suggested structure (particularly for groups who are new to implementing security measures as part of their strategy), you should feel free to focus on any part of the content which you feel is useful.

Each of the Sections is divided into a number of shorter Chapters, the majority of which are accompanied by one or more reflective exercises which should help you to get to know the relevant content in your own context. These exercises can often be used for individual reflection, but were written in such a way that they could also be carried out in larger groups. Tips are included to help you facilitate the exercises in a group setting.

For effective implementation within a collective or organisation you will need to regularly and consistently set aside time and space to work on you security and well-being as a group in the context of your activism.

The manual was written by an editorial collective of security and strategy trainers, in collaboration with a large group of experts and human rights defenders; as a result, the structure reflects that which would be utilised in a training scenario. The exercises in each Section provide space for reflection as individuals or groups, in order to facilitate a self-directed path towards holistic security practice without the necessity for external training and expertise. We invite you use this manual to guide and inform your holistic security practice at a pace suitable to you and/or your organisation.

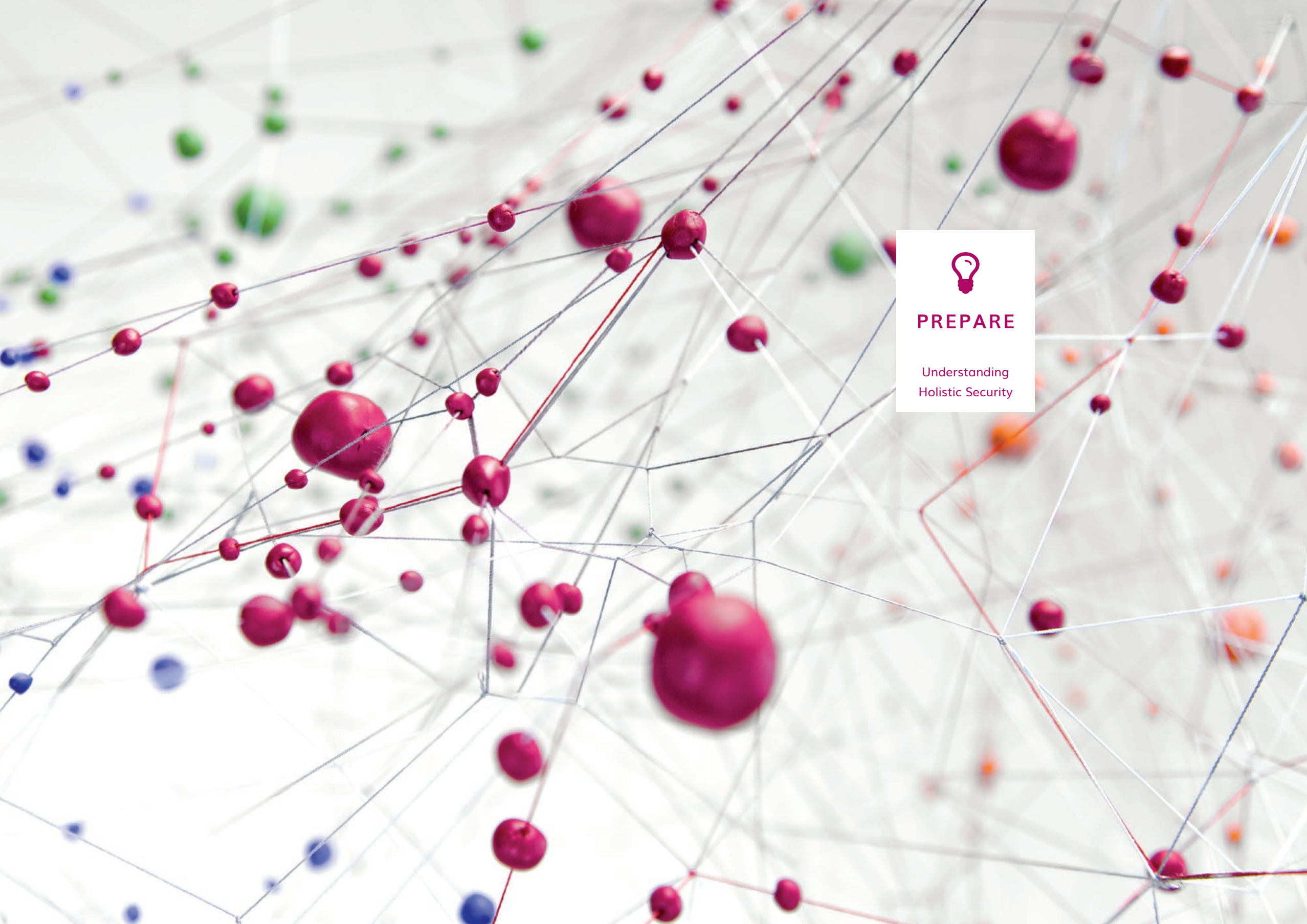
The intention and motivation behind creating and integrating a defined holistic security approach, in the sense of 'well-being in action', is to treat this as an iterative, evolutionary process wherein this manual is to be viewed as a starting point only. As such, the authors prioritised completion and thoroughness over making a shorter pocket guide; it is our hope that this longer text can later be contextualised to fit different audiences with differing priorities and preferred means of learning. Therefore, the authors whole-heartedly encourage feedback, contextualisation, copying, further development and wider distribution of such versions of this initial framework.

The manual builds on concepts previously established in a number of existing resources including Protection International's **'New Protection Manual for Human Rights Defenders'**[2], Front Line Defenders, **'Workbook on Security for Human Rights Defenders'**[3], Front Line Defenders and Tactical Technology Collective's **'Security in a Box'**[4] and Kvinna till Kvinna's **'Integrated Security Manual'**[5]. As such, we express our gratitude to the authors of the above guides, the community of human rights defenders and those working for their protection and empowerment. We hope that this manual contributes positively to the field.

Finally, we would be deeply grateful for any feedback or suggestions regarding how to improve the manual and its methodology, particularly those from human rights defenders and trainers attempting to implement it in the course of their work. Please, do not hesitate to contact us at ttc@tacticaltech.org with comments and suggestions which we can take into account in future editions.

---

2 http://protectioninternational.org/publication/new-protection-manual-for-human-rights-defenders-3rd-edition/
3 https://www.frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk
4 https://securityinabox.org
5 http://integratedsecuritymanual.org



PREPARE

Understanding
Holistic Security

I Prepare

Understanding Holistic Security

Contents

Introduction

In this Section, we will take the first steps towards adopting an organised holistic approach to our security as human rights defenders. In order to do this, we will first explore what the notion of 'security' actually means to us as human rights defenders, and consider the aspects of it which may not have occurred to us before. What is 'security', and what does it mean when we regularly put ourselves in danger in order to fight peacefully for what we believe in?

Although we may want to better organise our approach to security, we are never starting from scratch, but rather building on our existing well-being, attitudes, skills, knowledge and resources, which we will explore in this Section. Within this we will consider the personal beliefs which colour our perception of the world and can be important resources when we are under threat, as well as the instinctive responses our bodies have evolved to respond to threats, which we must recognise in order to better understand ourselves.

When we suffer threats to our security, the dynamics of the groups and organisations in which we operate can change in a number of ways. In this context, we will explore here some best practices for communicating about security as a peer-group, team or organisation.

In Prepare, we will:

- define what **security** means to us
- explore what we mean when we refer to **holistic security**
- reflect on our **existing security practices**
- learn about **natural reactions** to danger, and their advantages and limitations
- explore some **team, peer and organisational responses** to threat
- highlight best practices for **communicating about security** within groups and organisations.

1

What is Holistic Security for Human Rights Defenders?

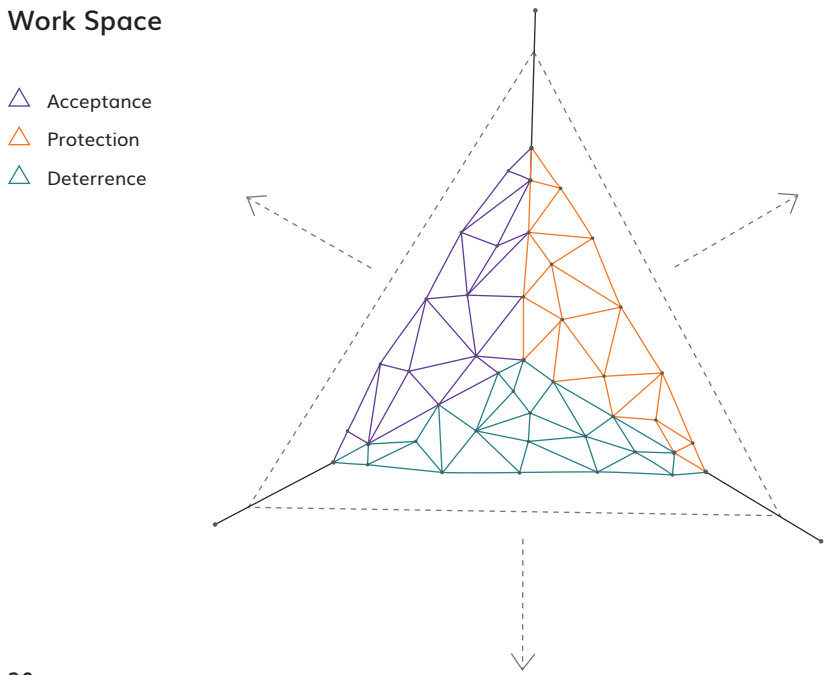
All of us desire and need a sense of security, the feeling that we are protected from harm. When we feel safe, we can relax our bodies, calm our minds, rest and recuperate. If we are unable to feel safe for extended periods, it is possible for us to quickly become tired, miserable and even physically ill. As human rights defenders, we sometimes choose to sacrifice our sense of safety (at least temporarily) in the pursuit of a better society, free from oppression and exploitation. Unfortunately, in the course of our work as human rights defenders, we are occasionally confronted by others who will try, perhaps through violence, intimidation and harassment, or by more subtle methods of oppression, to prevent us from achieving our goals.

Maintaining and expanding our space

Incidents ranging from arrests, intimidation and violent attacks, to harassment, reputational attacks, surveillance and social exclusion, can all be viewed as attempts made by our adversaries (those who don't share our aims or actively oppose them) to limit or close the spaces in which we work and live. These 'spaces' can mean literal physical spaces, including public squares and areas where groups can protest or demonstrate, our offices or homes, as well as our economic space (by limiting our access to resources), our social space (by limiting our freedom of expression or peaceful association), our technological space (through censorship, surveillance and access to our data), our legal space (through judicial, administrative or bureaucratic harassment), our environmental space (through promotion of 'development' models which are not sustainable), to name but a few.

By adopting an organised approach to security, our ultimate aim is to defend our space for work and, ideally, expand it so that the societies and States in which we operate will move with us towards respecting and protecting human rights.

In order to do this, we can adopt various tactics and utilise tools and weave them into plans for our human rights activities. These tools and tactics often correspond to one or more strategies for maintaining and expanding our space for work: those which encourage others to **accept** our work; those which **deter** attacks against us, and those with which we **protect** ourselves.



These over-arching strategies are expanded upon in more detail in **Section III | Strategise**.

Well-being as subversive and political

The threats faced by human rights defenders are varied and complex. We are perhaps used to thinking about security in rather narrow terms such as protecting ourselves from violent attacks, office raids, judicial harassment or threats from armed groups.

While an organised approach to these kinds of threats is indeed necessary, a holistic approach to security goes beyond that. Threats may also include structural forms of violence and harassment: economic and other types of marginalisation, extremely heavy workloads, lack of financial security, stress and traumatic experiences among a host of other factors. Such threats not only affect us, but also have implications for the people around us, including friends and family. Further, we must recognise that external threats affect not only our physical safety but also the space within ourselves, our bodies and our minds which, when threatened, inhibit our capacity to carry out our work and be content doing so. Well-being is central not only to carrying out our activism effectively but also to our ability to think as 'objectively' as possible, analyse and strategise.

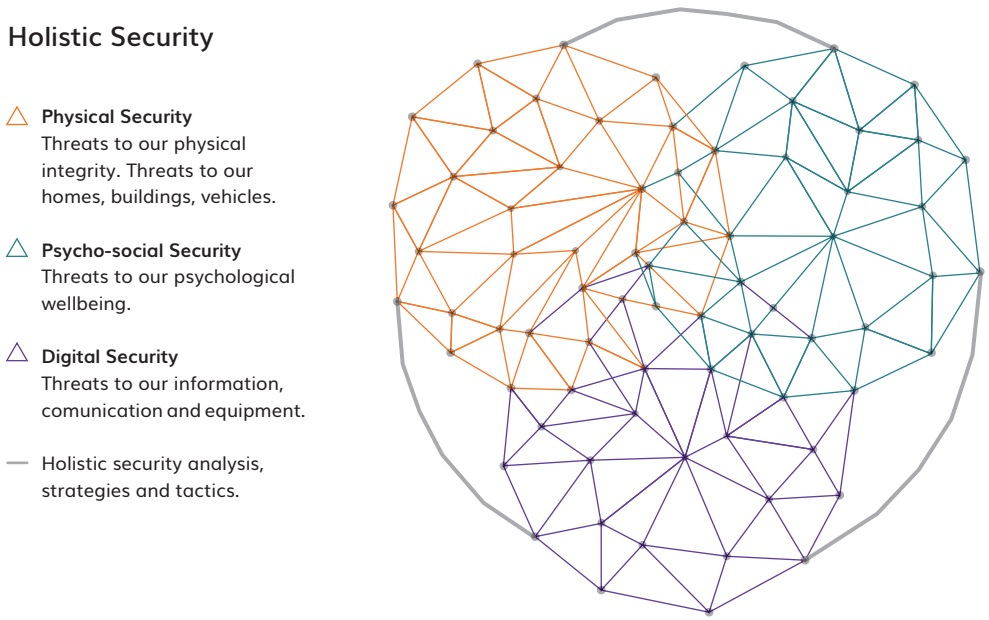
A holistic approach to security understands self-care not as selfishness, but as a subversive and political act of self-preservation. How we define our well-being in the context of activism is subjective and deeply personal. It is influenced by the differing needs of our bodies and minds, the challenges we face, our beliefs (religious, spiritual or secular), our gender identities, interests and relationships. As activists and human rights defenders, we must define security for ourselves and build solidarity and support for one another into our groups, organisations and movements on this basis.

In spite of threats to our space for work and personal expression, we don't often give up: we decide to keep challenging the injustices which we see in the world. For this reason, **we can think of security for human rights defenders as well-being in action**: being physically and emotionally healthy and sustaining ourselves while continuing to do the work that we believe is important, and carrying out the necessary analysis and planning to stay secure on our own terms.

Taking control of our information

No organised approach to security is complete without an organised approach to information and data management. The tools we rely on to manage our information – digital and analogue – also form part of our space for work and are subject to many of the same threats which we face in other areas.

Largely unseen and operating behind closed doors, the surveillance industry has experienced huge growth since the turn of the century. Access to our sensitive data (the files we manage, our email and mobile phone communication, etc.) is ever more important to those seeking to hinder the work of human rights defenders. Equally, the digital dimension now comprises a huge part of our lives, yet many of us feel that it is not within our control or treat it as something which does not impact our 'real' security. We must challenge these perceptions; identifying our sensitive data, understanding where it is stored and who has access to it, before undergoing a process of implementing means to protect it is not only a security measure, but also an act of political self-empowerment.



Holistic security practice, therefore, refers to the conservation of the well-being and agency of ourselves as human rights defenders, our families and communities, through the consistent use of psycho-social, physical, digital and other tools and tactics in ways that reinforce (rather than contradict) each other. These tactics enable us to increase our overall security, mitigate the threats we face and expand the choices we are able to make on a day to day basis.

Resilience and agility

It is worth bearing in mind that the threats and challenges in the world around us are always changing. This is particularly true for human rights defenders.

We must avoid falling into the trap of thinking that we can plan for everything. Unfortunately, due to our work, 'unexpected' events are almost the norm for many of us and activist communities need to be able to develop the necessary emotional and mental flexibility to deal with this. Cultivating a strong sense of well-being and feeling mentally and emotionally centred, is critical in a context where the risks and threats that we encounter are largely unpredictable.

Given the needs and demands of activism that can destroy even the best laid security plans, a more realistic approach is not to ignore the unexpected but instead to incorporate it into our responses. In this sense, it is not sufficient to simply develop a security plan and follow it to the letter. Rather, it is better to work with the unexpected and develop other attributes such as presence of mind or centredness to sharpen our ability to cope with it.

We often continue to carry out our work in full awareness of the threats that come along with it. Indeed, it is our own vulnerability that keeps us connected to the experiences of others whose rights are being violated. It is not possible to make ourselves completely 'safe' and perhaps it is not even desirable. With this in mind, we also need to build **resilience** and **agility**. Resilience is the ability to recover quickly from set-backs or injuries. Agility is the ability to quickly adopt new security practices in response to new or emerging threats. The goal is not to be safe through doing nothing, but to consciously face threats and protect ourselves and our communities as much as possible, so that we can still be engaged and active.

For most human rights defenders at risk, the notions of resilience and agility are not new, nor is the idea of having tools and tactics for staying safe during dangerous work. In this first exercise, we will explore some of the existing practices we have for staying safe.

Note: The exercises throughout this manual can usually be done alone or in a group. In some group settings the topics addressed may be sensitive or divisive. It is therefore important that you create a 'safe' space where everyone in the group feels comfortable speaking and sharing their own opinions and there is a general atmosphere of trust. Some tips on how to create a safe space include establishing shared agreements at the beginning of the conversation, being mindful that it's OK to have differing opinions, making sure that all members of the group are heard and that each person's contribution is treated as equally valid.

1.1 Exercise

Reflection on existing security practices

Purpose & Output

This exercise helps you reflect on what security means to you and explore the security tactics, plans and strategies that you consciously or unconsciously have in place.
You get a snapshot of your existing practices, how they interact with each other and how you can use it as a foundation for the next steps.

Input & Materials

If you want to document the results, write the answers on a flip-chart or sticky notes on a wall.

Format & Steps

Individual reflection or group discussion

Ask yourself or the group the following questions:

1. Think about the word 'security' or 'safety'. What does it actually mean to you? What do you need in order to feel secure or safe?
2. What do you do every day to avoid danger and protect yourself, your property, your friends or family?
3. When was the last time you did something which made you feel safe and strong?
4. Call to mind an activity you carried out which was dangerous. What did you do in order to stay safe?
5. What other people are important in helping you to feel secure or safe?
6. What resources or activities are important in helping you to feel secure or safe?

Take note of your answers to these questions as they will be useful in later exercises and Sections of the guide and will remind you that you are not building new practices from 'scratch'.

Remarks & Tips

Colleagues or team members might feel strange talking about 'security' if there is no existing organisational culture of talking about these issues. This exercise can nevertheless be utilised to start such a process of awareness raising.
The exercise itself might start the process of generating ideas on what to improve or add to your security practices. You might want to take notes on these in preparation for **Section III | Strategise** which deals with planning.

As activists, we may pay little conscious attention to security, and only passively note the absence of danger or feeling insecure. By referring to holistic security as 'well-being in action', we propose to be more conscious about security from an empowering perspective and to create an integrated experience by grounding security in our daily perceptions of threat and security, our feelings, reflections and practices shaped by the communities in which we live and work.

In the rest of **Section I | Prepare**, we begin preparations for a more comprehensive and organised approach to security. We start with an examination of how people react to danger and threats on a physiological level and in what ways this affects our perceptions, mindset, and subsequent actions. We then explore working in teams and groups while being under stress and danger and how positive (and negative) dynamics emerge in this context which will influence our security.

2

Individual Responses to Threats

Organising our approach to security is largely about developing a more accurate ability to perceive and analyse threats and choose means of avoiding them. However, we need not develop this perception from scratch: we already have physiological responses to threats which should be understood and acknowledged. Furthermore, our perception and ability to analyse may be challenged by some aspects of our work. If we are at least aware of these, it will help us plan more realistically.

People have natural defence mechanisms which developed through our evolution. Hard-wired into our brains are neural pathways and structures with the primary function of keeping us alive when we are threatened. These functions are most often below the level of conscious awareness; that is, our security processes are operating even if we are not aware of them. This applies both when we ourselves are under threat, or indirectly, when someone close to us is threatened.

One of our survival mechanisms is often called intuition, those powerful but seemingly irrational feelings that we sometimes have about a particular person, place, or activity. When our intuition is signalling untrustworthiness or danger, it is often because we have picked up multiple, subtle **indicators** which alone do not identify a particular threat, but taken together strongly suggest the presence of danger. Many human rights defenders have been saved by paying attention to their intuition or 'trusting their gut', even when they could not explain how they knew they were in danger.

Intuitions of danger produce a feeling of **anxiety**. Although anxiety is an uncomfortable feeling, it is an extremely helpful one. Anxiety provokes us to act to reduce our discomfort. When we feel anxious we actively seek out information that might confirm or challenge the possibility that we are in a potentially harmful or dangerous situation. Depending upon what we learn, our anxiety might develop into fear.

When we feel fear we demonstrate powerful **survival responses**. These responses are driven by the same brain structures and supported by biological changes. When this happens much of our behaviour becomes automatic, in the sense that we have less conscious awareness of choosing to act in a particular way. Common survival responses include the following responses.

1. **The 'freeze response'** is when a person becomes utterly still while remaining highly alert and poised for action. This response relies on escaping notice until the danger has passed. For example, we might cease the work that we are doing, stop communicating through our usual channels, or reduce communication with someone with whom we are in conflict. In each case, we are hoping that the unwelcome attention will pass if we become inactive.

2. **The 'flight response'** is when a person quickly tries to get as far away from the danger as possible. We might move our operations to a safer location, abandon certain activities or modes of communication, or separate ourselves from people who might cause us harm.

3. **The 'comply response'** involves doing what an aggressor instructs in the hope that co-operation will result in the attack ending quickly and with less injury. We might agree to suspend or abandon certain objectives or activities, or give up passwords to secure information.

4. **The 'tend response'** happens when people try to protect other, more vulnerable people who are being similarly victimised. Many human rights defenders are motivated to help others because of our own experiences of oppression and exploitation.

5. **The 'befriend response'** involves trying to build some kind of relationship with the aggressor in the hope that this will limit the harm perpetrated against oneself or others. By telling physical aggressors about our families, we might try to humanise ourselves in their eyes, a strategy that is sometimes useful in reducing violence.

6. **The 'posture response'** is an attempt 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. **The 'fight response'** is when a person attacks with the intent of driving off or destroying the aggressor. Of course there are many different ways to fight and we all make our own choices about this.

It is important to note that when engaged in a survival response, we become quicker, stronger, more focused and more resilient than we would normally be. As a result, these survival strategies are extremely effective in many circumstances. It helps to remember that even though you might only be beginning to develop your own organised approach to security, your natural survival mechanisms are already hard at work.

As powerful as our survival responses are, they are not perfect. While our brains are capable of processing enormous amounts of information and reacting very quickly, they do not do this in a systematic and logical manner. There are some situations in which our brains are particularly untrustworthy, and we should pay special attention to these.

Threats from the digital sphere

One of the ways in which we can be let down by our physiological responses discussed above relates to digital and information security. We are well adapted to respond to physical threats (such as defending ourselves from attack), or interpersonal threats (such as coping with estrangement from family members) and as a result we have strong intuitive and emotional reactions to these kinds of danger.

However, whilst our physical and digital worlds are closely interwoven, we can struggle to identify or respond appropriately to digital attacks; a suspicious stranger standing outside our home might make us very anxious and prompt us to take action to make ourselves safer, yet clear warnings of viruses on a computer are more likely to be experienced as irritants, and ignored or even disabled, despite having very real implications.

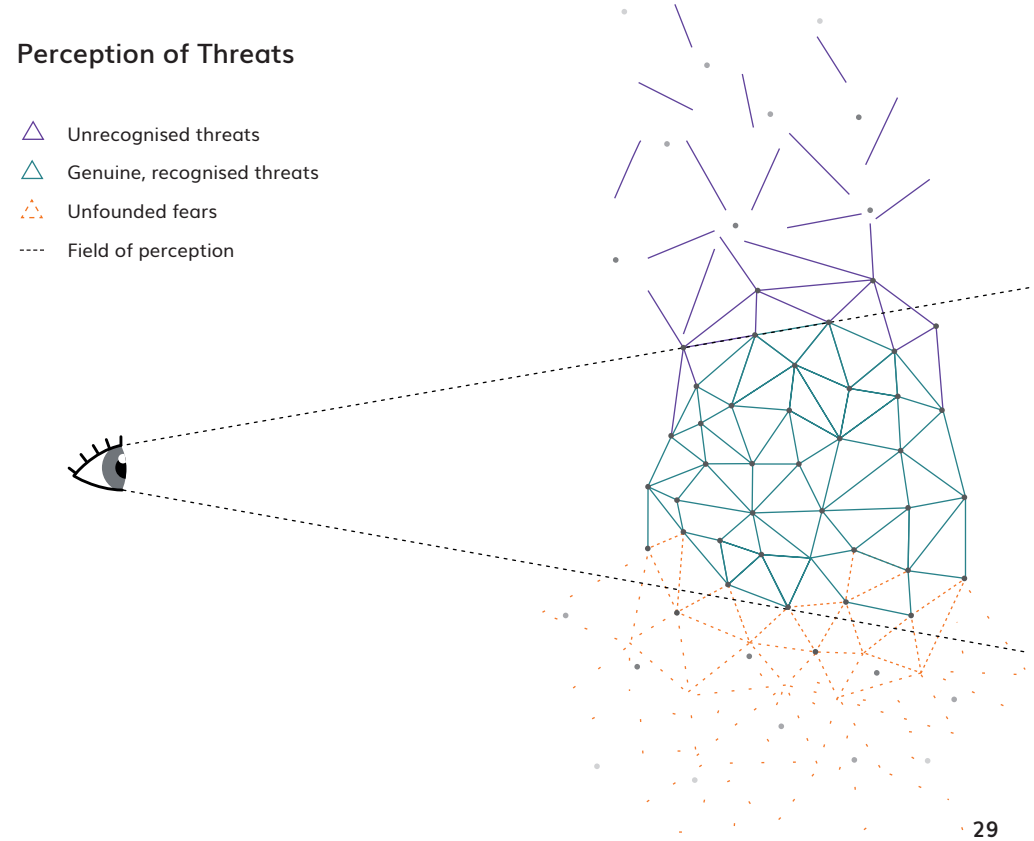
Moreover, the prevalence of proprietary technology and the secrecy surrounding electronic surveillance make it difficult to establish what threats we face. Frequently we fail to recognise these threats, or conversely we perceive threats which may not actually be relevant to us.

Since human rights defenders are subjected to ever more sophisticated means of electronic surveillance and depend more than ever on digital tools, we must learn to make up for this lack of protective instinct. Through taking account of our information as an important asset in our work and opting to protect our data from unwanted access or surveillance where we deem it necessary, we can increase our levels of certainty and reduce the stress and fear which this topic may cause us.

Trauma, stress and fatigue

Very disturbing or **traumatic past experiences** may unhelpfully distort the way we respond to indicators of danger. This is particularly true of those traumatic experiences that stay with us in powerful and uncomfortable ways, even years after the event. These kinds of traumatic experiences lead to two common reactions. For many people, past traumatic experiences contribute to our **unfounded fears**. These people become over-sensitive to things that remind them of past traumatic experiences. When this happens, entirely harmless situations take on a sinister appearance and our intuition begins to tell us that we are in danger when we are not. This can lead us to having reactions which are inappropriate and impact our relationships with the people and organisations around us.

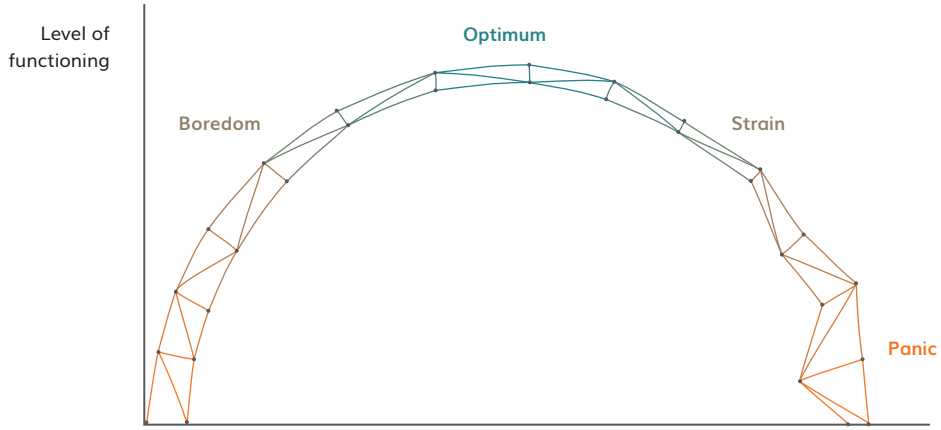
Other people recognise their problem or become exhausted by continually having their brains and bodies reacting to these false alarms. Over time, these people sometimes start to suppress or ignore their healthy internal alarm system. While this helps people live more effectively in the world, it does also reduce their awareness of potential threats in the environment. In this way, past traumatic experiences may contribute to **unrecognised threats**.



Stress and fatigue can also result in us inaccurately identifying and responding to indicators of threats in our environment. When we feel overwhelmed by the challenges in our work and home lives, or when we have been working too hard, for too long and without enough rest, we start to behave differently.

Every person has a level of challenge or threat that stimulates them to a point of maximum productivity and well-being. If there is not enough stimulation and challenge in our lives, we feel bored and become unproductive, even depressed. If there is too much challenge or threat, we start to become overwhelmed. We feel that we cannot cope with everything that life demands of us, and once again we become unproductive, anxious and depressed.

Stress Curve



Many human rights defenders may be accustomed to high levels of challenge in their lives, and some may even enjoy it, but this doesn't mean that we are impervious to stress. Each of us has a limit after which we can no longer cope. When this limit is reached, we become unhappy and our productivity suffers. Furthermore, the level of care and attention that we give to our security drops.

When we are over-worked, security indicators can sometimes be seen as just one more problem we have to deal with. If our coping resources are already completely committed, we might choose to ignore the indicator or react in ways which

are not helpful to ourselves, our colleagues or our work. Another reason for failing to deal adequately with real threats is that we become accustomed to a certain (and sometimes growing) level of threat in our personal or work life. This level of threat starts to feel 'normal' or comfortable. When this happens, we are less likely to take steps to improve our safety.

As a result, developing a culture (both individually and as a group, organisation or movement) of stress management and self-care is fundamental to a holistic approach to security. Not only will this help to prevent threats brought about through long term exposure to stress and fatigue, but it will greatly aid critical thinking about security in general.

In the following exercises, we will reflect upon some of our past experiences and how these may continue to affect our perceptions of danger. Once we are more aware of this, it will be easier to build tactics for keeping our perception 'in check' in our security planning.

1.2a Exercise

Self-awareness exercise: Recognising and reacting to threats

Purpose & Output

The purpose of this exercise is to help you recognise the areas in which your perceptions are most accurate and the areas in which you may be less clear-sighted.

You should gain a clearer understanding of:

- your reactions to threats in the past which went well and not so well
- the gaps in your recognition of threats
- things you may want change
- things which make you confident facing new threats and should be continued.

Input & Materials

Printed copies of the questions

Format & Steps

Individual reflection

Think back on a past experience where you felt particularly unsafe and then acted to take care of yourself. While the experience might have been primarily physical, emotional or related to information security, it might also have had additional impacts on other aspects of your security.

Use the following table to keep track of your insights.

Remarks & Tips

It is helpful to take time for this exercise and write your answers clearly so that you can come back to them as you deepen your self-awareness. If you do this, take care to keep your notes in a private place, sharing your personal thoughts and questions only with people that you trust.

Choose one moment when you felt threatened or in danger and then acted to protect yourself. Consider experiences of physical danger (such as a robbery), emotionally damaging experiences (such as being threatened or betrayed) or threats to your information and communications (such as devices being confiscated or telephones being wire-tapped.

How did you become aware of the threat?

Were there earlier indicators of the threat that you noticed, or maybe failed to notice? Consider indicators in the socio-political environment, in your physical environment, in your devices and in your body and mind.

Were there earlier indicators of the threat that you had noticed, but dismissed as unimportant? Consider indicators in the socio-political environment, in your physical environment, in your devices and in your body and mind.

What were your initial reactions when you became aware of the threat and how effective were these?

What were your subsequent actions and how effective were these?

What would you change if you could go back in time? What would you do instead?

What can you learn from this experience which might help you feel more confident in your ability to cope with future difficulties?

1.2b Exercise

Note: If you, your team members, colleagues or fellow activists have gone through traumatic experiences and you want to know how this might impact your perceptions of threats, you can run this deepening exercise. This exercise may be more emotionally challenging so if you do not presently feel ready, consider completing it at another time.

Self-awareness exercise: How traumatic experiences affect our perception

Purpose & Output

The purpose of this exercise is to help you recognise areas in which your perceptions are most accurate and areas in which you might be less clear-sighted due to traumatic experiences.

Input & Materials

It is helpful to take time over these questions and to write down your answers clearly so that you can come back to them over time and as you deepen your self-awareness. If you do this, take care to keep your notes in a private place, sharing your personal thoughts and questions only with people that you trust.

Format & Steps

Think back on any past traumatic experiences that may not be fully resolved. These will be experiences that you think about often and which still have the power to make you feel frightened, angry, guilty, ashamed, or sad. Don't go into the actual situation, but focus on what you did to help yourself, what you did to help others and what others did or might have done to help you.

Consider the following questions:

- What kinds of dangerous situations are particularly emotionally loaded for you as a result of your past experiences?
- When you find yourself in potentially dangerous environments, are there any situations that make you anxious or scared quite easily?
- Is there someone you trust who could help you identify any unfounded fears you may have?
- What kind of threats do you feel you fail to recognise easily?
- How might you check whether you are failing to recognise some indicators of danger?
- With whom do you feel comfortable discussing your fears and possible blind spots?

Remarks & Tips

As this exercise might prove to be emotionally challenging, communicate this clearly to your colleagues. It is important that nobody feel coerced into participating in this exercise, and if someone starts to become distressed, they should stop immediately. It might also be a good idea to relate it to other activities, which cover areas of psycho-social well-being.

Optional Exercise: Use of Time[6]

As human rights defenders, a very important aspect of our lives which we often lose track of is our use of time. Our workloads are often extremely difficult to manage and our struggle to stay on top of them may come at the cost of our physical and emotional well-being. It may also have a negative effect on our ability to perceive dangers. You can explore this for yourself in the exercise below.

The development of successful security practice demands the commitment of resources, most notably time. As individuals, we need time to reflect on the effect our work is having on us, to ask questions and find answers, to identify successful tactics and tools, to plan and co-ordinate and to integrate new practices into our lives and work.

6 Reproduced from Barry, J. (2011) Integrated Security: The Manual, Kvinna till Kvinna Foundation, Stockholm.

Feelings of emotional security are often related to our use and perception of time. What is the ratio between our working or engagement hours and the time we spend with our loved ones or for recreational activities? As activists, we nearly always face the dilemma that our workload never ends but our energies do. So where do we draw the line? The "Use of Time" exercise from the Integrated Security Manual helps us to make conscious steps towards a healthier and more emotionally secure use of time, which you can find in **Appendix E.**

3

Inner Beliefs and Values

Our instinctive physiological responses are not the only resource we have at our disposal to help us build resilience when facing threats. Understanding ourselves and our security in this context also demands that we reflect on the values and beliefs we bring to our activism: they inform how we perceive the world and society around us, our role within it, and indeed our understanding of security and well-being. From this perspective, it is helpful to recognise the inner beliefs and values which inspire us, motivate our work and build our resilience. It is equally important that we respect the values and beliefs of our colleagues and fellow human rights defenders in order to avoid contributing to division, tension and mistrust in our collectives, organisations and movements.

The inner beliefs and values that underpin our work vary greatly. For some, they may have their roots in traditional cultural, religious or spiritual beliefs; for others, they may be entirely humanist or atheist. In any case, for many human rights defenders, inner beliefs and ethical values are a fundamental lens through which we perceive the world: they offer many of us a sense of purpose; they can help us find inner peace in times of turmoil, strength in the face of adversity and healing when hurt.

However, these values are often deeply significant and personal, and we might hesitate before voicing them to others. We think about bringing our values to our work as a personal process, but what does it look like to be explicit about our values as individuals, or indeed our common values as a collective or movement? If we articulate our ethos, beliefs and their associated rituals, and recognise the role these values play in inspiring our activism and maintaining our resilience, we will be more inclined to create, respect and defend space for them within our work.

Conversely, it may also be the case that we assume (correctly or incorrectly) that our colleagues or fellow human rights defenders share the same values or beliefs as we do. Acting on the basis of these assumptions, we can inadvertently limit the space for the distinct values and beliefs of others during our work together. Regardless of what values or beliefs underpin our work, it is beneficial to forge a group environment in which we can be confident that the values that motivate us are respected and perhaps even celebrated.

A first step towards a more comprehensive view of our values – be they atheistic, spiritual, religious or otherwise – is to create a safe space where we can share them with those around us. This can prove a communal source of mutual understanding, inspiration, growth and support, paving the way for us to better understand why, as activists, we take the risks we take, and enabling us to better care for each other in the course of our work.

Further, such a space must be open and respectful, wherein each person feels able to share the values which inspire them in a way which does not lead to judgement, arguments or dogma, but rather fosters solidarity, mutual respect and learning.

Faith and cultural practices as a source of connection or division

As much as faith and cultural practices can be a unifying or connecting factor within your team, they can also become the opposite. If minority practices are discouraged, for example by not taking dietary requirements (which may be cultural, ethical or religious) into account when organising group meals or creating an atmosphere of 'us and them', they can become a divisive force. This negatively impacts not only those who are marginalised, but the entire group.

Looking at wider society, faith and cultural practices could form a unifying (and perhaps strategically useful) connection between you and the society you want to transform. However, it could also become a divisive factor, which separates you from the 'others', and could be exploited to stigmatise or target you.

For a closer look at these connecting and dividing factors, and how you can impact them, see Section III | Strategise. The Do-No-Harm Approach.

So far we have discussed holistic security in terms of individuals. Nevertheless, as human rights defenders, we seldom work alone and most of us have families and communities which may also be directly or indirectly affected by our work. Commonly, we work with peers and in groups. As groups, we need to build sufficient trust to talk to each other meaningfully about our motivations and fears, to develop a shared understanding of the risks and threats facing us, to agree an integrated set of security practices, to build solidarity, resilience and agility together and to hold each other accountable for consistently implementing those practices. We will explore the dynamics of these relationships in the context of our work in the next Chapter.

4

Team and Peer Responses to Threats

People organise themselves into groups such as families, circles of friends and teams – both within and outside our human rights activism. When people feel anxious or frightened, these groups may change in ways which are at least partly predictable. Since achieving holistic security almost always involves other people, it is helpful to think about how groups change in times of increased danger: this will aid our planning process. Below, we explore a few examples of how group dynamics can be affected by threats such as harassment, marginalisation, physical and other forms of violence (such as economic, gender-based, institutional, or structural violence).

Harder group boundaries

One predictable change that occurs to groups subjected to threat is that the boundaries that define the group become solidified: people within the group become more closely connected to each other and those outside the group become more distant. It also becomes more difficult for people to join or leave the group. While the protective functioning of such changes is important, there are also some potential difficulties with this. Harder boundaries may distance the group from existing and potential allies, leaving it more isolated than it might otherwise be. They also reduce the flow of information into and out of the group,resulting in members of the group being less informed than they might otherwise have been, and having fewer opportunities to check their perception of the world against that of others. Harder boundaries also make it difficult for people to leave groups. Members who wish to leave might be branded traitors or sell-outs in a way that is harmful both to that person and others perceived to be his or her allies. It is very helpful for groups to regularly discuss the ways in which people and information enter and leave the group, and how to manage this in a holistic way that truly promotes our security.

Fixed patterns

A second predictable change is that the patterns of behaviour become more fixed and harder to change. This makes it more difficult for a member of the group to question supposedly shared beliefs, or challenge the behaviour of other members. When we lose the ability to question each other's assumptions or point out potentially unhealthy behaviours, our ability to constructively and compassionately build group security is greatly compromised. For this reason, it is important that groups regularly revisit and discuss their shared values in an honest way.

Authoritarianism

A third predictable change relates to leadership and power dynamics within groups. When groups feel unsafe, group members tolerate greater authoritarianism from leaders or more powerful members of the group. This results in less information exchange within the group, and fewer opportunities for group members to check their perception of the world with other members of their team. In extreme cases, powerful members of the group may become abusive, and the increased rigidity of group boundaries may prevent victims from leaving. Again, it is important for groups to talk about power dynamics and leadership styles on a regular basis, and to make sure that every person has an opportunity to contribute.

Looking at the links between decision-making and security, we should not underestimate the positive effects of having fair and transparent decision-making processes. The danger of adversaries targeting leaders of a group is less pronounced if a group has shared responsibilities and knowledge.

Different groups can, however, respond in different ways: it is a good idea to consider how your group or organisation responds to the pressures of working under threat and the impact this has on each individual's well-being in the group. This demands an openness to the possibility of talking about security in the group, which we will explore in more detail in the next Chapter.

Mistrust and infiltration[7]

Suspicion and mistrust within and between groups of human rights defenders is common and may or may not be justified depending on the circumstances. Often, it has its roots in the tactics of infiltration and spying which are frequently used against human rights defenders, although merely creating suspicion and mistrust can also be a primary objective of our opponents.

In a context of oppression, people become informants for many reasons: they themselves are often victims too. Therefore while carrying out our work, we may occasionally be suspicious of others in our movement or organisation. There are many cultural, sub-cultural and interpersonal reasons for this mistrust, including observed 'suspicious' behaviour of the person in question, and our own perceptions and subjective criteria about whom we trust.

This suspicion comes at a price paid in mistrust and fear. The potential benefit of perhaps outing an informant in the group may not protect us from other informants present. Furthermore, the atmosphere created by a 'witch-hunt' mentality can drain the energy and motivation of the whole group. It may be due to this atmosphere, that we falsely accuse a colleague of spying, which could in turn prove more damaging than actually having an informant in the group.
It is often useful to create an open discussion within the group and agree on a transparent process for deciding on how sensitive information is to be treated, and how to deal with members of the group who may be disruptive. It might be helpful to review your decisions on secrecy or the transparency of your activities in light of the possibility that there are informers in your group. Creating space to talk about fears linked to the possibility of informers in the group, or group members being pressurised to become informers might prevent situations of witch-hunting or demonisation of informers.

Infiltration of human rights organisations and movements often has the ultimate aim of either documenting or – more often still – provoking illegal activities.

7 Based on: Jessica Bell and Dan Spalding Security Culture for Activists. The Ruckus Society, www.ruckus.org/downloads/RuckusSecurityCultureForActivists.pdf

In this regard, it is useful to ensure that the activities of the organisation or group in defence and promotion of human rights are explicitly of a non-violent nature, protected under international law and standards such as the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), and the International Covenant on Economic, Social and Cultural Rights (ICESCR) among others. In this case, those in the group who push for illegal or violent methods of protest or civil disobedience should be treated with caution and their membership of the group reconsidered.

The question of infiltration is a complex one involving many different variables and much uncertainty. Many of the tools described in **Section II | Explore** of this manual are useful in helping human rights defenders carefully think through the problems of possible infiltration.

In the next Chapter, we will learn some helpful strategies for creating and implementing a regular space for talking about security within organisations.

5

Communicating about Security within Teams and Organisations

Once we understand how individuals and teams react to stress and threats, it becomes important to reflect on how healthy practices towards this can be fostered in our groups and organisations.

Creating a safe and regular environment for communicating about security within teams and organisations is one of the most important preparatory steps towards a successful security strategy and organisational well-being. All of the tools outlined in this and other resources which help us build our security demand time and space to be made for speaking, exchanging, reflecting and learning about security. Aside from this clear practical necessity, creating space to talk about security with our peers and colleagues helps us to:

- more accurately perceive the threats to our work (reduce unrecognised threats and unfounded fears)
- understand why members of the team might react differently to stress or threats (individual responses to threats)
- assign roles and responsibilities for security measures
- increase group ownership of security measures
- build solidarity and care for colleagues who are suffering from threats.

However, there may be barriers that prevent us from discussing security openly within our organisation. Some barriers may include:

- heavy workloads and lack of time
- simply being afraid to discuss it
- a sense that our observations on security might be perceived as fear, paranoia or weakness
- not wanting to confront colleagues about their practices
- not wanting to be the first to bring the matter up for discussion
- gender issues and/or power dynamics.

In order to create a space for discussion, we can engage in the following:

a. building trust within the team

b. regularly scheduling talks about security

c. fostering a healthy culture of interpersonal communication.

As we explore each of these, we will discuss ways to establish them, and some of the benefits (as well as the disadvantages) associated with each of them.

a Building trust within the team

Having a team that operates based on trust is optimal for productivity as well as for security purposes. Trust facilitates the implementation of new security measures, especially among members who could not be, or were not involved in making the decisions about it. It creates an atmosphere of openness in which members will more readily share their security incidents and the information they feel is important, and even their mistakes. It gives members confidence to know whom to talk to about which aspects of security.

There are several ways we can work on increasing trust within a team. Below are some examples of activities to accomplish this:

- Getting to know each other outside the professional or activist context, e.g. through out-of-work activities, socialising and having fun.
- Checking regularly on the well-being of team members (perhaps as a start to team meetings), to have an idea about everybody's stress levels, general mood and what they are bringing to their activism from their personal lives.
- Transparency about hierarchies and decision-making structures.
- Clear protocols for how to deal with personal or sensitive issues that may arise including (but not limited to) security incidents, threats and so on.
- Having access to a counsellor or trusted psychologist.

Building trust within a team is not a trivial task – it involves investment and taking risks, given the potential for infiltration noted above. However, in this regard, aside from trust in one another, we can also build trust in our strategies for managing sensitive information, clear channels and create means for communication about it.

An atmosphere of trust also relies on everyone being able to give and receive constructive criticism and feedback, which will be explored in the segment on interpersonal communication below.

b Encouraging regularly scheduled talks about security

As explored in **Chapter 1.4 Team and Peer Responses to Threat**, it is essential to create regular, safe spaces to talk about the different aspects of security. When a team sets regularly scheduled time aside to talk about security, it elevates the

importance of the topic and the conversation. This way, if team members have concerns around security, they will be less anxious about seeming paranoid or wasteful of other people's time.

Scheduling regular talks about security also normalises the frequency of interaction and reflection on matters relating to security, so that the issues are not forgotten, and team members are more likely to bring at least a passive awareness of security to their ongoing work.

It is also important to incorporate security elements into the normal functioning of the group. As such, we avoid making security an extraneous element, but rather an integral part of our strategy and operations. For example, this can be achieved by adding security to the agenda of a regular meeting. Another way is to rotate the responsibility for organising and facilitating a discussion on security between members the group, so as to instil the notion that security is everyone's responsibility and not just that of a select few.

In situations of high risk, it is important to increase the number of check-ins at meetings and informal spaces, as well as raising group members' overall receptiveness to talking about security in a supportive atmosphere.

In the next exercise, you will find some questions to help you explore the culture within your group in regard to talking about security, identifying barriers and considering ways to deal with them.

1.5a Exercise

Talking about security in groups and teams

Purpose & Output

The purpose of this exercise is to reflect on how and when we talk about security with our peers, colleagues or team. It is best facilitated by at least two people, but can also serve as a useful individual reflection on your interaction with your colleagues.
This helps start a process to constructively talking and discussing security in your team/group.

Input & Materials

To do this exercise in a participative way and in order to document it, you may need writing material (cards or stickies and markers). A large area of wall-space, a flip-chart or pin-board may also be useful.

Format & Steps

Individual work & group discussion

Step 1: Divide the group into pairs. Ask each pair to consider the following questions concerning group dynamics and write down their answers.

- What topics take up the majority of time in group conversations?
- What topics do we never seem to find time for?
- What aspects of our group interaction do we find energising?
- What aspects of our group interaction do we find exhausting?
- What happens in the group when people disagree?
- Have you created any space to develop and refine your own security practices (as an individual)? Describe it: where and when does this space exist? Is it sufficient, and how might you expand this space, if necessary?
- Do you have enough space to talk about security issues with others, such as peers or colleagues who work closely with you, and how might this space be created or expanded if necessary?

Step 2: Collate the full set of responses to these questions on a board or in a notebook.

Step 3: As a team, consider the following questions.

- Where and how do we want to set our priorities concerning security?
- What are common problems that arise around talking about security as a group?
- What can prevent us from talking about security? How can we deal with this?
- How can we create and maintain sufficient and adequate space for talking about security? What will this mean in terms of time and resources?
- How might we increase the effectiveness of our group interaction on security?
- What problems arise around committing to changing our security practices? Do we resist change, individually or collectively, and why?

Format & Steps

Step 4: Invite each person individually to reflect on:

- Whether you should have a similar awareness for your family and loved ones?
- What are the differences in the dynamics and ways in which family and loved ones are affected?
- In what ways do you communicate the threats you are facing to your family, community, friends and others not in your work circle?

Step 5: In the whole group, share the points that people feel free to share. Then you should agree on what can be communicated to those 'outside' the group, for reasons of confidentiality, intimacy and security. Agree on these guidelines for the whole group.

Remarks & Tips

Consider also discussing the steps and requirements necessary to put your ideas of how to talk about security in the future into practice.

Important questions to consider might be:

- What happens if you don't progress on 'talking about security'?
- What happens if someone does not stick to the guidelines on what can be communicated to the outside?

C Fostering a healthy culture of interpersonal communication

Individuals' ability and willingness to engage in open communication with each other is fundamental to creating a space where security can be frankly and effectively discussed.

We must make sure that communication among team members stays healthy and open, so that we have access to as much information as possible and can make more informed decisions, as a group, about our security.

Talking about security can, however, be challenging for a number of reasons, due to its very personal nature and the fact that our vulnerabilities and even mistakes are often very relevant information. Finding a constructive way to talk about security in groups or organisations helps avoid misinterpretations that can lead to conflict between the people involved.

Below are some aspects worthy of consideration in creating a healthy culture of communication:

Prevailing atmosphere around security

It helps to come to terms with what the existing (organisational) mindset around security is. For instance, we can reflect on whether the time allocated to talking about security is as valued and tended as other meeting times; or we can pay attention to whether group members are dismissive in voice and tone when discussing security matters; or if we are genuinely interested and personally connected when our colleagues are addressing their concerns.

Existing hierarchies

It is also important to create mechanisms for such communication across hierarchies within an organisation, so that members are able to discuss things in an atmosphere free of power dynamics.

Communication under stress

Paying attention to our communication style within teams becomes particularly important during times of increased stress. In times of threat and stress, we tend not to focus on our language and tone due to other extenuating circumstances. We may not even be aware of our impatience, or we may expect others to understand the reason behind our change in behaviour.

Intercultural situations

We also have to bear in mind that communication is a fundamental aspect of culture and cultural diversity. We should pay attention to our verbal and non-verbal communication in intercultural situations.

Formal modes of communication

Some groups tend to be more formal in communication and about decision-making in meetings. While formally establishing practices for security and well-being is useful in many contexts, this mode of communication can occasionally hinder open sharing, especially regarding the emotional aspects of security. Thinking about facilitation and formats for these discussions may help arrive at an effective structure that provides space for open sharing of hopes and fears, as well as for more technical discussions. It is important to incorporate all of these aspects when making decisions about security.

One example of a useful practice in interpersonal communication is through the method of **non-violent communication**. Non-violent communication is a method of communicating based on the assumption that all people are compassionate by nature, that we all share the same basic human needs and that each of our actions is a strategy to meet one or more of these needs.

While this method is certainly culturally shaped in the 'West', it allows for communication to include ways of comfortably reflecting on how the communication is affecting everyone involved. This can be especially effective for giving and receiving feedback about security and in discussing the impact of attacks, accidents, threats or other security-related events on us as individuals and groups.

A major advantage of employing such a particular way of structuring conversations and feedback is that it helps avoid accusatory manners of expressing views and encourages clarification where there is misunderstanding. In the following exercise, you can practice following the steps for giving constructive feedback on security according to the basic principles of non-violent communication.

1.5b Exercise

Non-violent feedback

Purpose & Output

The purpose of this exercise is to practice non-violent communication as a means of improving the effectiveness of communication about security within teams and groups. It provides for a reflection on how we can give our feedback in an understandable, clear way and avoid some of the pitfalls which can lead to arguments or ineffective communication.
The exercise is best carried out in pairs at first, although it can be adapted for larger groups.

Input & Materials

It may be useful to write the guidelines for non-violent feedback somewhere visible, like on a flip-chart.

Format & Steps

Decide on a setting for conducting a feedback discussion (this can be done in pairs, or with observers, taking turns). The participants should choose a topic (real or imaginary) about which they want to give feedback. This can be a security-related topic, such as an incident which took place already, or something else entirely.
Ask the person giving feedback to follow the guidelines below. For each guideline, a small illustrative example is given. Here, we are imagining a scenario in which two colleagues are talking: one of the colleagues often works late and once forgot to lock the door of the office when leaving; the other colleague wants to talk about the incident.
The recipient of the feedback should only ask questions of clarification but not comment, reply, justify or question the content of the feedback.

Guidelines for non-violent feedback:

I speak for myself: You can only speak from your own subjective experience – not about 'common sense', 'my group', 'we', or 'one', but only 'I'.

- e.g. "I felt unsafe when I found the office unlocked this morning".
- Bad practice: "What you did yesterday put us in danger!"

What did you observe? You should speak only of the facts as you experienced them, so the interlocutor knows what your feedback is referring to (what you saw, heard, etc.).

- e.g. "When I arrived at the office this morning, the front door was unlocked and I could open it without the key".
- Bad practice: "You forgot to lock the door yesterday!".

What was your reaction to it? What were your internal feelings and physical reaction to your experience? Try not to be judgemental, but again, simply speak from your experience as you understand it.

- e.g. "I was very worried, because I thought maybe we had been robbed. When I found that everything was OK, I was still quite angry."

How do you interpret it? What does your personal interpretation bring to the facts? Although your personal interpretation is indeed subjective, it is still valuable and colours your experience.

- e.g. "I think it happened because you have been working very late and were tired and simply forgot to close it"

Format & Steps

What are your wishes, advice, or interests? What are your suggestions for change based on this experience? They should be offered without demands, but rather as requests for consideration by the group.

- e.g. "I would feel better if I knew we were all getting enough rest and not overworking so that we could better take care of things like this, so it would be better if you didn't work so late".

Ask the pairs to then share their insights on the process and manner of giving feedback – not about the content. Did they experience different feelings than when they normally receive feedback?

This exercise can also be used to clarify the content and tone of your feedback as a preparation for an actual feedback session or potentially difficult discussion.

Remarks & Tips

It is important to receive feedback with your ears and not with your mouth, and understand it as a personal reflection from your partner, not as 'the truth' or an invitation to justify or defend your actions. You decide yourself if it is valuable to you and how to react to it. Following such an approach might be a preventive step for conflicts within your team. As such, it can contribute to your overall well-being.

If you are interested in deepening modes of communication which deal sensitively with conflict, you might want to have a look at non-violent communication approaches.

Be aware that 'speaking for myself only' is not appropriate in many regions around the world. Adapt the methodology so that it fits your needs and setting.

Conclusion

Hopefully, these exercises will have helped you get a better sense of what security means to you, as well as a better understanding of the way you and those around you respond to threats to yourselves and your work. Establishing a healthy culture of communication as explored above may represent one of the more difficult changes to make in adopting a more positive and organised approach to our security and well-being. However, understanding this and all of the topics covered in this Section is vital in order to make space for the process of context analysis, a key set of activities in improving and maintaining an organised approach to security, which we will expand in **Section II | Explore**.

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.

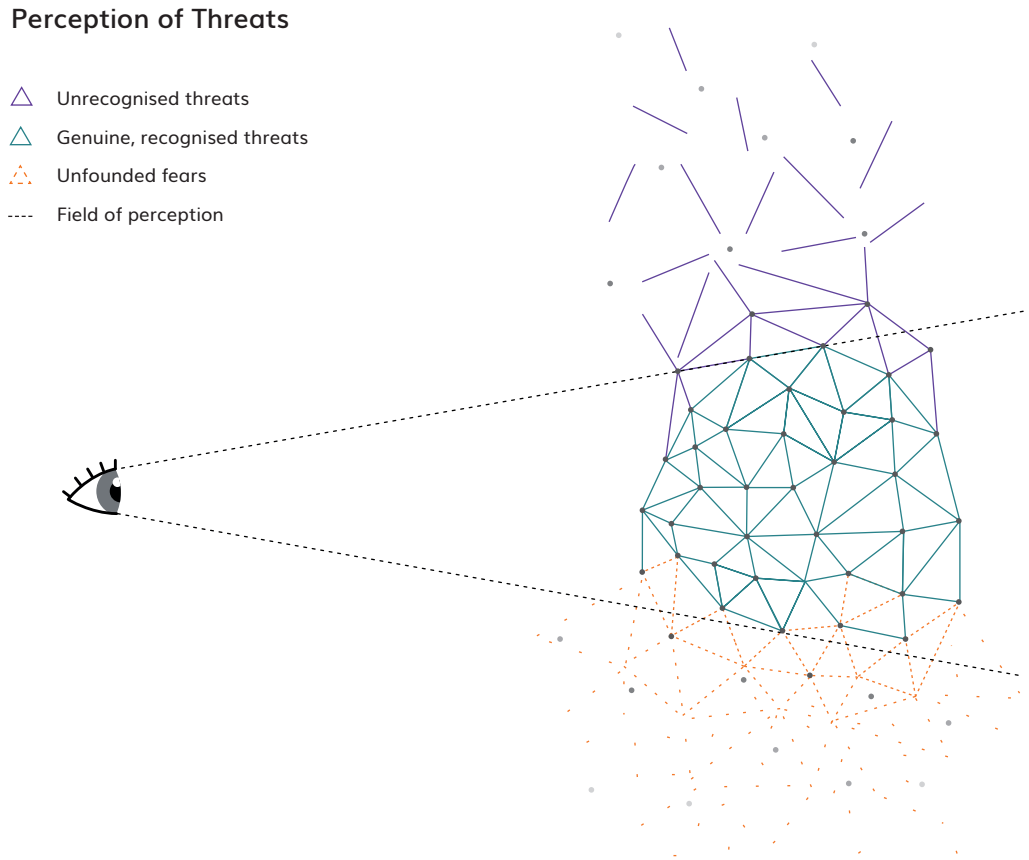
6. **Threat identification and analysis** — Attempting to drive off the danger by pretending to have greater power than one actually does. As human rights defenders, we often threaten to expose and publicise threats of violence so as to publicly embarrass our adversaries.

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.



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

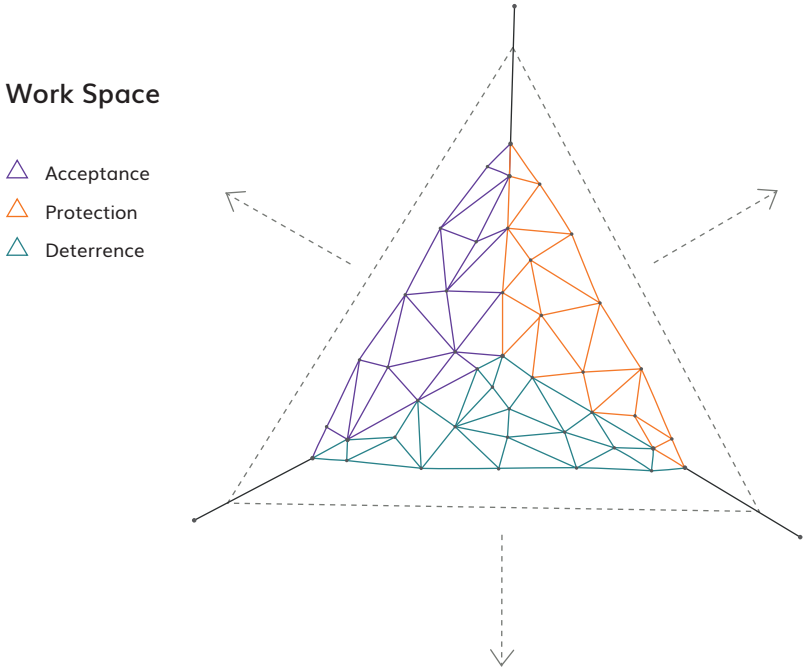
Once we have established our vision, we must consider the methods we can employ to realise it. We may carry out very diverse activities as individuals or organisations in order to achieve our goals. What are your 'areas of work' or the activities you carry out?

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

Format & Steps

target-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

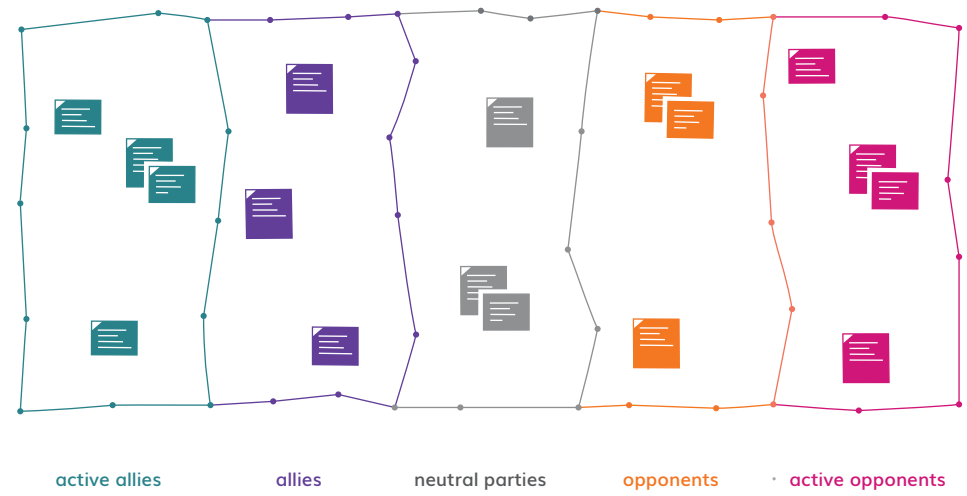
Once we have established the actors in our environment, it is helpful to categorise, to the best of our knowledge and ability, the nature of the relationships between ourselves and these actors, especially their stance regarding our vision, their interests and the amount of resources at their disposal.

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

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

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).
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.

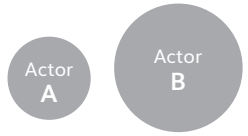
Examples of relationships to include here are:

- **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.

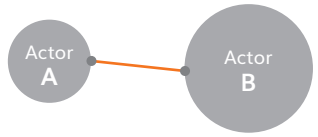
Remarks & Tips

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.

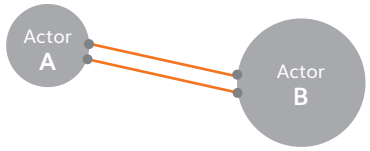
Legend[9]



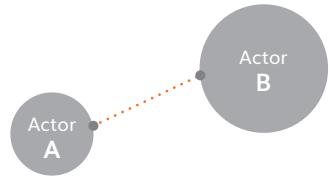
Different sized circles represent differences in power



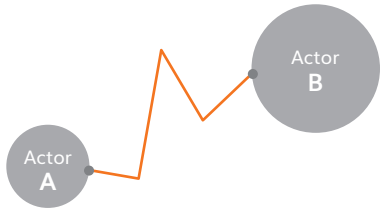
A solid line represents a close relationship
You can also 'break' the line (by crossing it in the middle) if there is a broken relationship



A double-line represents an alliance

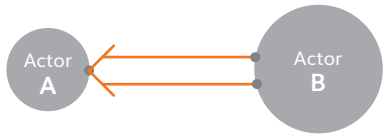


A dotted line represents a weak or unknown relationship

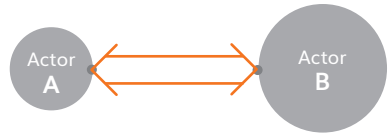


A jagged line represents conflict or a bad relationship

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

9 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.[10]

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.

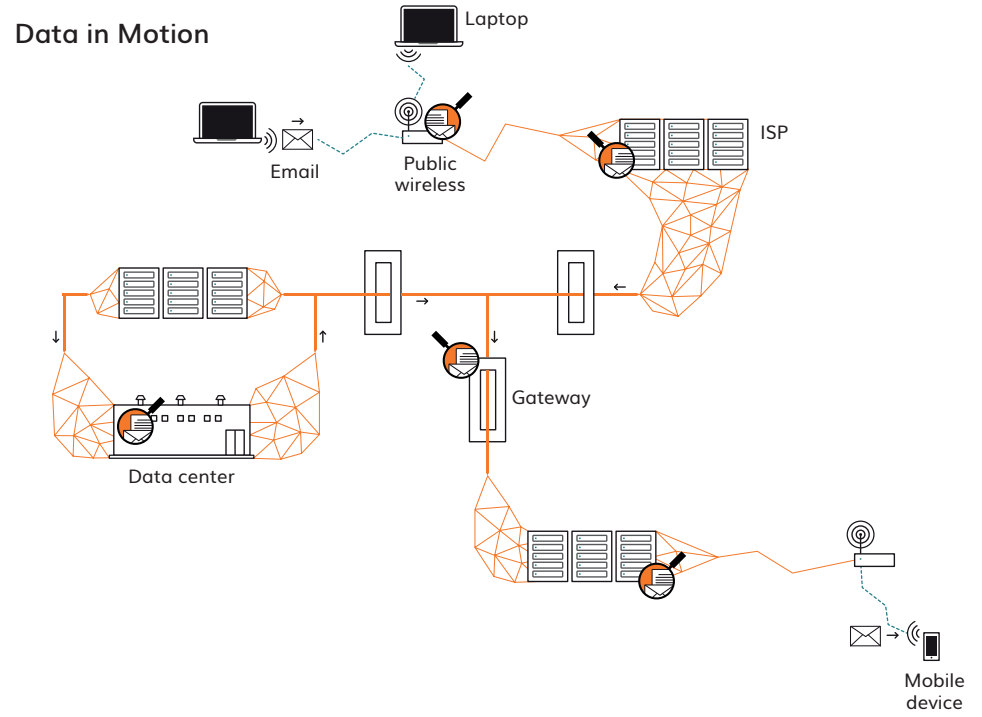
10 See https://mat.boum.org

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.



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[11]), 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.[12]

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

12 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 themselves, 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 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** earlier 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.[13]

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.

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

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

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[14]

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?

14 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

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:

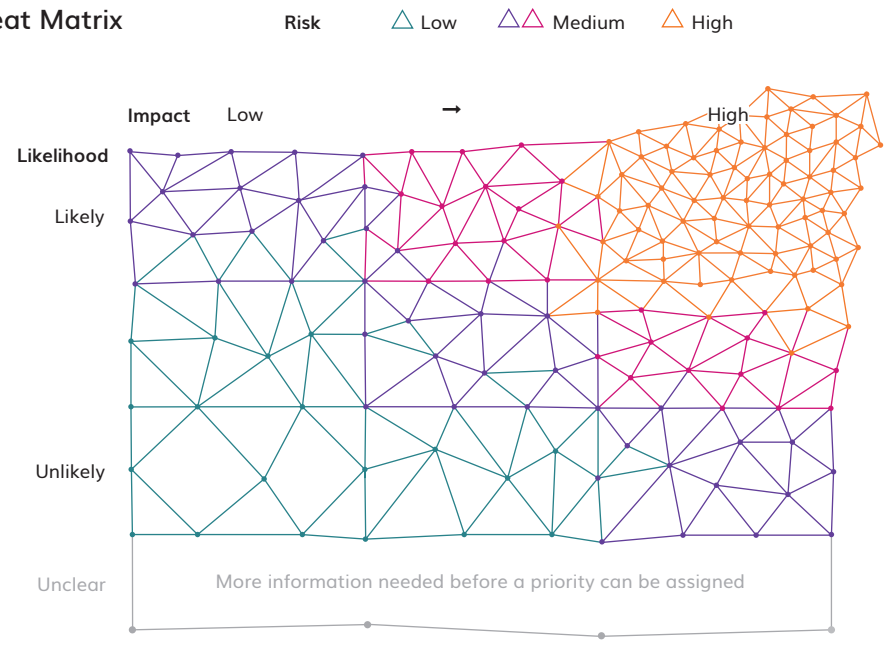
- How many people are affected?
- How long-lasting is the effect?
- To what extent does this hamper our normal operations?
- What other harmful situations does it enable?
- Is there an immediate danger to other people still not affected?

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.[15]

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 C.**

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.

15 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 or 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.

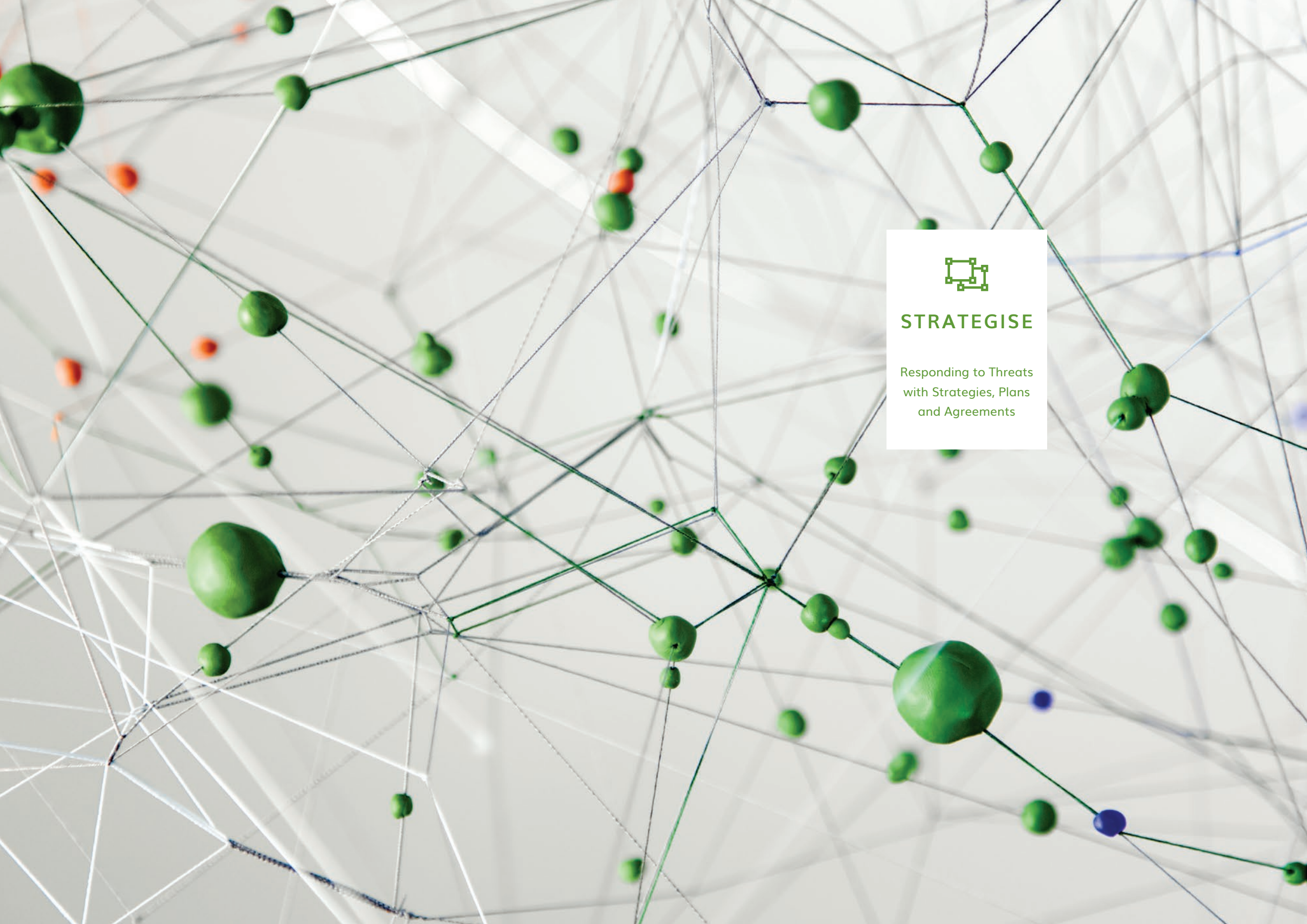
Remember that the above list is not a static list, and revisiting the process is very important. Shifts and changes in the context invariably affect the landscape of your work. Unforeseen threats may develop, or the likelihood of certain threats may be reduced due to external factors. You can determine 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.



STRATEGISE

Responding to Threats with Strategies, Plans and Agreements

III Strategise

Responding to Threats with Strategies, Plans and Agreements

Contents

Introduction

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

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

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

In Strategise, we will:

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

1

Analysing our Responses to Threats

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

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

Overall framework: Threats, capacities and vulnerabilities

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

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

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

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

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

Our existing practices and capacities

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

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

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

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

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

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

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

3.1a

Exercise

Existing practices and capacities

Purpose & Output

In this exercise, you can consider each of the threats you already identified and prioritised in light of your existing security practices and other capacities relative to them.
This will give you a 'baseline' on which you can later build and improve.

Input & Materials

To carry out this exercise, you need to have identified and prioritised threats in **Exercise 2.6b/c**.
It may be helpful to write out the the capacities you identify so you can review them later.

Format & Steps

Return to the threats identified in **Exercise 2.6b**. For each of the threats you have identified, there were a series of questions. Here you can relate your existing security practices and capacities to each of these questions as follows:

- **Who/what** is under threat? Identify here what capacities (if any) are already protecting this person or thing from this threat. Examples of capacities could include
  - in the case of judicial harassment: good legal knowledge
  - in the case of computer confiscation: having encrypted hard drives.
- **Who** is behind the threat? Do you already have some kind of tactic for engaging with this actor? Are there any tactics or

Format & Steps

resources you have leveraged in order to prevent them from acting against you? If so, what? If they have acted against you before, did you respond in some way? If so, how? If you don't have any, that is fine: this will be important to remember when you identify gaps.

- **How:** What information is necessary for them to carry out the attack? Do you have any information protection or counter-surveillance practices in place which might prevent that information from falling into their hands?
- **Where:** What access to you or your property do they need? How do you secure the physical spaces around you (e.g. buildings, vehicles, private property) in order to protect yourself and your property? For example, do you lock your offices and homes? What 'common sense' practices do you have for your personal safety in dangerous environments? All of these are important to note, so that you don't start from zero!
- **Psychological, emotional and health tactics:** Include any well-being practices that are in place to deal with this threat – do you have any practices which help to reduce stress, tiredness etc., and increase centredness and awareness which may help respond to this threat?

Where possible, try to consider these aspects relative to each of the threats you have identified. **If you can't think of an answer for one or more of the questions, that is fine:** you have just identified a gap to be filled! You will consider gaps in the following exercise, and use them as a way to identify what new resources and practices you need.

Remarks & Tips

Caution! For each of the answers you give, consider **whether this practice or capacity is positive. How do you know?** There is a slight danger of creating a false sense of security if you falsely credit an existing practice with helping to keep you safe. If you are not sure about something, it would be worth taking the time to think over and **talk to your colleagues or trusted friends** in order to get a fresh perspective.

If you wish to record the results of the exercise in writing, you could use a format like the one below:

Threat	[Title of the threat]			
Summary	[Brief description/summary of the threat]			
What	**Target**	**Adversary**	**How**	**Where**
Describe what happens if the threat is carried out (if required, subdivide the threat into its components below).	Specify what/who is the target.	Who is the entity behind this threat?	What information is necessary to carry out the threat?	What are physical spaces in which the threat can manifest?
1)				
2)				
3)				
Psychological, emotional and health impacts				

Identifying gaps and vulnerabilities

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

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

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

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

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

3.1b Exercise

Vulnerabilities and gaps in our existing practices

Purpose & Output

In this exercise, you can consider each of the threats you identified and prioritised in **Section II | Explore**, in light of the gaps in your existing security practices and your vulnerabilities. This will give a much clearer picture of where you need to begin building new capacities.

Input & Materials

To carry out this exercise, you need to a) have identified and prioritised threats in **Exercise 2.6b**, and b) collated the output from **Exercise 3.1a** above.

Use pens and paper or other writing materials.

Format & Steps

Return to the threats identified in **Exercise 2.6b** and the existing capacities and practices you identified in **Exercise 3.1a**.

Here, you can attempt to identify the gaps in your existing practices and your vulnerabilities, relative to each of the questions you answered previously. Consider the following questions:

- **Who/what** is under threat? Identify here what gaps or vulnerabilities (if any) are making this person or thing more vulnerable to the threat. Vulnerabilities could include:
  - in the case of judicial harassment, a person having little legal knowledge, or
  - in the case of computer confiscation, the hard-drives having no password or disk encryption.
- **Who** is behind the threat? What vulnerabilities or gaps exist in our ability to influence this actor? For example, if there is no way of directly engaging with the actor to create acceptance of your work or deter an attack, this could be considered a gap.
- **How**: What information is necessary for them to carry out the attack? Is it difficult to control the flow of information – are there any vulnerabilities in the way you deal with information relevant to your work that may facilitate this threat or make it more damaging?
- **Where**: What aspects of the physical spaces around us (e.g. buildings, vehicles, private property) may make this threat more probable or more damaging? In the case of an office raid and theft, for example, having weak locks on the doors would be a vulnerability.
- **Psychological, emotional and health vulnerabilities:** in the context of this threat, how might stress, tiredness etc. affect you? What gaps or vulnerabilities exist in your well-being practices that may make this threat more likely, or more damaging?

If you wish to record the results of the exercise in writing, you could use a format like the one below:

Threat	[Title of the threat]			
Summary	[Brief description/summary of the threat]			
What	**Target**	**Adversary**	**How**	**Where**
Describe what happens if the threat is carried out (if required, subdivide the threat into its components below).	Specify what/who is the target.	Who is the entity behind this threat?	What information is necessary to carry out the threat?	What are physical spaces in which the threat can manifest?
1)				
2)				
3)				
Psychological, emotional and health impacts				

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

Identifying new capacities

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

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

3.1c

Exercise

Brainstorming new capacities

Purpose & Output

In this exercise, you can consider each of the threats you identified and prioritised in **Section II | Explore**, your capacities and your vulnerabilities in order to identify the new capacities you need to build in order to maintain your well-being in action.

Input & Materials

To carry out this exercise, you need to have identified and prioritised threats in **Exercise 2.6b**, and the outputs from **Exercises 3.1a** and **3.1b** above.

Format & Steps

Reflect on the threats you face and your existing capacities and vulnerabilities identified in the previous exercises. You may want to write down your answers in a format such as in **Appendix D.**
Here, you will attempt to 'brainstorm' the new capacities you want to build. Consider the following questions which may help you identify them:

- **Who/what** is under threat? What new capacities should the person or people under threat build in order to reduce the likelihood or impact of the threat identified?
- **Who** is behind the threat? How might you try to influence the cost-benefit analysis of the people or institution who might be behind the threat identified? Is there any way you can improve their tolerance or acceptance of our work, or deter them from acting against you?
- **How:** What information is necessary for them to carry out the attack? How can you further protect the sensitive information about your work and prevent it from falling into the wrong hands?

Format & Steps

- **Where:** How can you increase the security capacities of the physical spaces around us (e.g. buildings, vehicles, private property) in order to make this threat less likely or damaging?
- **Psychological, emotional and health considerations:** In the context of this threat, what practices can you build to reduce stress and tiredness in order to be more aware and react more creatively to the threat?

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

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

2

Building New Approaches to Security

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

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

Security strategies: Maintaining a space for our work[16]

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

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

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

Some find it helpful to categorise these strategies as follows:

Acceptance strategies

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

Protection strategies

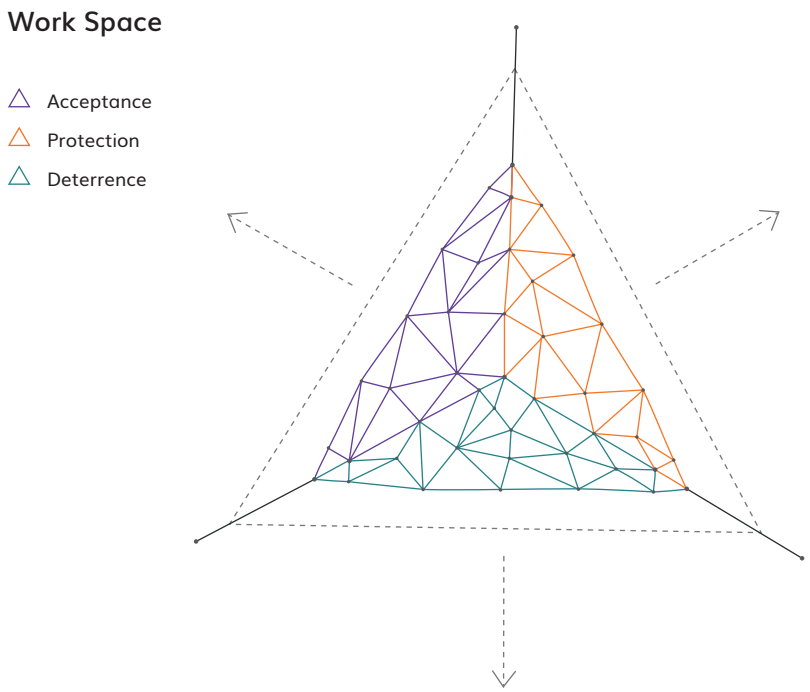
A protection or self-defence strategy emphasises learning new methods and implementing new practices or leveraging the strength of your allies to protect yourself and cover the gaps in your existing practices. Examples of practices which fall into this category might include implementing the use of email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

---

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

Deterrence strategies

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



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

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

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

Capacity building

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

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

Well-being

If we want to learn anything new or undergo any process of change, we need to create the conditions in our body and mind to facilitate this process. This implies not only self-care in a physical and psychological sense but also means creating the necessary time and space in our daily schedules and consciously incorporating the learning processes into our routine, instead of seeing it as an additional burden to our existing workloads.

Attitudes

are the extent to which we or those around us are open to the idea of changing our practices and see such changes as logical, necessary and valuable. Attitudes are subjective and can – like our perception of threat – be adversely affected by the experience of stress, fear and trauma. In **Section I Prepare** you can find more information about fostering positive attitudes in ourselves and our groups towards security.

Knowledge in this case refers to our understanding of the world around us, and in a practical sense, our knowledge of the political, economic, social, technological, legal and environmental context which impacts our security. In **Section II | Explore** you can find a series of steps which can be taken to improve our knowledge of our context from a security perspective.

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

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

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

3.2a Exercise

Acceptance, deterrence and protection tactics

Purpose & Output In this exercise, you can further develop the new capacities you have identified as necessary to improve your security. Thinking about them in terms of acceptance, deterrence and protection strategies will help you get a sense of your overall security strategy and help you come up with additional tactics to develop.

Input & Materials If you want to write down the results of the exercise, consider using a format like the one in **Appendix D.**

Format & Steps

Step 1: Look at the new capacities to build that you identified in **Exercise 3.1b.** Consider whether each of them is:

- an acceptance tactic
- a deterrence tactic
- a protection tactic
- a combination of the above.

Step 2: Now, for each threat, consider further new tactics you could employ in order to:

- increase tolerance and acceptance of your work among your adversaries or society in general
- dissuade your adversaries from taking action against you by raising the cost of an attack
- protect yourself from threats and respond more effectively to them.

Continue to elaborate your list of new capacities with the new ideas you come up with.

Step 3: For each of the new capacities you have identified, consider the resources (financial and material) to which you will need access in order to build these capacities.

External resources for capacity building

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

External trainings and consultants

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

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

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

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

External consultants should not:

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

Tips on how to choose adequate trainings or trainers

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

Material resources for security

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

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

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

3

Creating Security Plans and Agreements

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

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

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

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

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

Elements of security plans and agreements

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

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

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

Both purposes are explained in more detail below.

Prevention of threats

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

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

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

Emergency plans

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

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

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

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

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

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

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

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

Well-being and devices

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

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

Objective

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

Threats

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

Prevention - actions and resources

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

Response - actions and resources

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

Emergency plan

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

Well-being considera-tions

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

Devices and information

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

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

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

4

Security in Groups and Organisations

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

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

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

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

Creating and maintaining security plans

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

Achieving buy-in

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

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

Participatory design

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

Role-playing

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

Re-planning and considerations

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

Emergency planning in groups and organisations

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

Definition of emergency

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

Roles and responsibilities

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

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

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

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

Channels of communication

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

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

Early alert and response system

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

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

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

Improving organisational security management

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

Assessment

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

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

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

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

- donors
- external consultants and trainers.

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

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

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

Criteria for assessment

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

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

Acquired security experience

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

Attitudes and awareness

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

Skills, knowledge and training

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

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

Security planning

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

Assignment of responsibilities

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

Ownership and compliance

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

Response to indicators

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

Regular evaluation

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

3.4 Exercise

Assessment of organisational security performance

Purpose & Output	This is a basic exercise which checks perceptions of members of the organisation regarding the implementation of organisational security measures
Input & Materials	Some drawing materials or a copy of the security wheel exercise (**Appendix E**)
Format & Steps	You may want to focus on overall organisational security performance, or one more specific aspect of your organisation's security practices such as digital security, psycho-social well-being, travel security, security in conflict zones, etc.

Step 1: Use the organisational 'security wheel' (**Appendix E**) or draw a circle and divide it into eight sections, each with a title (as in the diagram) to create your own security wheel.

Step 2: For each segment of the wheel, colour in a proportion which, in your opinion, reflects the extent to which your organisation implements best practices.

Step 3: For each segment, each person should identify the barriers which are currently preventing them or the organisation in general from better observing best practices

Step 4: Similarly, consider what the potential solutions are for each barrier or problem.

Step 5: Compare results among members of the organisations. Where is there consensus, and where are there differences? Why might that be?

Step 6: Together, try to identify areas which must be prioritised for improvement.

Prioritising areas for improvement

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

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

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

Overcoming resistance to security planning[20]

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

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

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

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

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

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

Common Resistance Stereotypes

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

Reasoning behind the stereotype

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

Responses to overcome resistance

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

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

Reasoning behind the stereotype

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

Responses to overcome resistance

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

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

Reasoning behind the stereotype

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

Responses to overcome resistance

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

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

Reasoning behind the stereotype

There are more important issues than security of defenders.

Responses to overcome resistance

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

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

Reasoning behind the stereotype

Security is expensive and cannot be included in fundraising proposals.

Responses to overcome resistance

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

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

Reasoning behind the stereotype

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

Responses to overcome resistance

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

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

Reasoning behind the stereotype

It is impossible to find time in the work schedule.

Responses to overcome resistance

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

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

Reasoning behind the stereotype

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

Responses to overcome resistance

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

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

Reasoning behind the stereotype

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

Responses to overcome resistance

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

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

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

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

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

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

Actions + Behaviours = Consequences.

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

Actions and resources

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

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

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

1 Competition vs. inclusivity

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

2 Substitution vs. appreciation

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

3 Selectivity and power relations

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

4 Standard of living and working

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

Behaviours and implicit ethical messages

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

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

1 Cultural characteristics

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

2 Different values for different lives

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

3 Fear, tension and mistrust

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

4 Use of resources

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

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

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

Conclusion

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

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

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

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

Further Reading

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

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

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

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

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

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

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

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

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

Bibliography

- Barry, J. (2011) Integrated Security: The Manual. A project of The Kvinna till Kvinna Foundation. Available at: www.integratedsecuritymanual.org

- Barry, J. and Nainar, V. (2008), Insiste, Persiste, Resiste, Existe: Women Human Rights Defenders' Security Strategies. A joint project of Urgent Action Fund for Women's Human Rights, Front Line Defenders and The Kvinna till Kvinna Foundation. Available at: http://kvinnatillkvinna.se/en/publication/2013/04/18/insiste-persiste-resiste-existe-2009/

- Bell, J. and Spalding, D., Security Culture for Activists. A project of The Ruckus Society. Available at: www.ruckus.org/downloads/RuckusSecurityCultureForActivists.pdf

- Bertrand, M., Monterrosas, E., and Oliveira, I. (2014) Programa de Asesorías en Seguridad y Protección para Personas Defensoras de Derechos Humanos. A project of Peace Brigades International Mexico Project. Available at: http://www.pbi-mexico.org/fileadmin/user_files/projects/mexico/images/News/Reducido_GuiaFacilitacion.pdf

- Camfield, J. and Tuohy, S. (2015) SAFETAG Manual. A project of Internews. Available at: https://safetag.org

- Cane, P. M., CAPACITAR Emergency Response Tool Kit. A project of Capacitar International. Available at: http://www.capacitar.org/emergency_kits.html

- CDA Collaborative, Do No Harm http://cdacollaborative.org/cdaproject/the-do-no-harm-project/

- Chenowith, E. & Stephan M. J. (2013) Why Civil Resistance Works, Columbia University Press.

- Davis, J. (2015) Security to Go: A Risk Management Toolkit for Humanitarian Aid. A project of European Interagency Security Forum (EISF). Available at: https://www.eisf.eu/library/security-to-go-a-risk-management-toolkit-for-humanitarian-aid-agencies/

- Eguren, E. and Caraj, M. (2009) Protection Manual for Human Rights Defenders, Protection International, 2nd Ed. A project of Protection International. Available at: http://protectioninternational.org/publication-page/manuals/

- Lakey, G., Spectrum of Allies. A project of Training For Change. Available at: http://www.trainingforchange.org/tools/spectrum-allies-0

- Martin, B. (2012) Backfire Manual: Tactics Against Injustice, Irene Publishing. Also available at: http://www.bmartin.cc/pubs/12bfm/index.html

- Rimmer, A. (2011), Workbook on Security for Human Rights Defenders. A project of Front Line Defenders. Available at: https://www.frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk

- Shields, K. (1993) In the Tiger's Mouth: An Empowerment Guide for Social Action, New Society Publishers. Social Barometer exercise available at: https://organizingforpower.files.wordpress.com/2009/05/allies-chart-new1.jpg

- United Nations Office of the High Commision for Human Rights (OHCHR), Declaration on Human Rights Defenders. Available at: http://www.ohchr.org/EN/Issues/SRHRDefenders/Pages/Declaration.aspx

- Voisin, J., MAT: Metadata Anonymisation Toolkit. Available at: https://mat.boum.org

Appendix A

How Do I Use My Time?[22]

Take some time to consider the way in which you spend your time. Reflect and write your answers to the following questions about your work, resources, coping mechanisms and health. You do not have to share the answers with anyone. If carrying out the exercise in a group, it may be interesting to reflect on how it felt to look at your use of time in this way.

1. Your work	hours/day	days/week	hours/week
a. In total, how many hours per day do you spend working as an activist (paid and unpaid)? How many days a week do you do this work? 'Work' in this sense can mean meetings (in or out of office), events, workshops, conferences, work chats, replying to emails, working from an office or from home, 'social' work events, consultations, etc.			
On average, how many hours per day do you spend on unpaid work (activism)? How many of days per week?			
On average, how many hours per day do you spend on paid work (activism)? How many of days per week?			
b. On average, how many hours per day do you spend on work that is not related to your activism (often your main source of income)? How many days per week?			
c. On average, how many hours per day do you spend on domestic chores (cleaning, administration, shopping, caring for others, etc.)? How many days per week?			

2. Your resources	hours/day	days/week	hours/week
a. Training: on average, how many hours per day do you spend on your training (this could include school, classes, library, courses, lectures, workshops, diploma courses, preparing for exams, thesis)? How many days per week?			

b. Nutrition: on average, how many hours per day do you spend eating?

How many times on average per day do you eat? .....

Do you frequently skip any meals in a day? .....

If yes, which meal? .....

Do you substitute any meals with 'fast food'? .....

If yes, which meals? .....

.....

.....

22 Based on material from Barry, J. et al. (2011) The Integrated Security Manual, Kvinna Till Kvinna. http://www.integratedsecuritymanual.org/sites/default/files/wriex_howdoiusemytime.pdf

c. **Exercise:** on average, how many hours do you spend doing some form of exercise per day?			
d. **Personal care:** on average, how many hours per day do you spend on personal care? How many days per week?			
e. **Rest:** on average, how many hours per day do you spend on quality rest (sleep or naps)? What time do you usually go to bed? What time do you usually rise?			
f. **Personal development/contemplative practices:** on average, how many hours per day do you spend on personal development (being with yourself, reflecting, meditating, other contemplative or spiritual practices, attending healing and/or therapy session)?			
g. How many hours per day do you spend on your **interpersonal relationships:** family, friends, partner/lover(s), others? How many days per week?			
h. How many hours per day do you spend on **pleasurable/relaxing/supportive activities**? How many days per week?			

List those activities here: .....

.....

.....

3. Health

a. When was the last time you visited a health professional/healer?	
b. How many times per year do you have a routine health check-up?	
c. Do you feel pain in your body right now? If so, where?	
d. If you have pain in your body, what steps do you take to ease that pain?	
e. If you have health concerns, what are they?	
f. If you do have major health concerns, have you brought them to the attention of a health-care professional with whom you feel comfortable?	
g. Any other health comments?	

Appendix B

Scanning Digital Devices for Security Indicators

The following is a non-exhaustive check-list of ways in which you can check your digital devices regularly in order to establish a base-line and note security indicators with greater ease.

Scanning devices for malware or spyware

For users of Windows and Mac OS computers in particular, it's important to regularly scan your devices for malware and spyware. For more information on this, see the Avast! and Spybot tool guides in Security in-a-Box.[23,24]

Checking your firewall

It's a good idea to become familiar with the settings of the firewall on your computer – and to install one if you don't have one already. The firewall helps you to determine which programs and services can establish connections between your device and the internet.

If you open your firewall settings, you should be able to find a list of which programs and applications can send and receive information to and from the internet. You may see many applications you don't recognise here: it is a good idea to search their names with a search engine to determine whether or not they may be harmful.

Checking the task manager

On Windows computers, you can open the task manager by pressing CTRL+ALT+DEL. This will open a list of all the programs and services which are running on the computer. If you see anything suspicious, you might want to do a web search to find out more about it. You can stop it by selecting it and clicking "end task".

Two-step authentication for accounts

Many online services such as Google Mail, RiseUp Mail, Twitter and Facebook allow users to set up "two-step authentication", which means that aside from knowing your password, you will need to enter a code sent to your mobile phone in order to log into your account. If you use this method, you will be alerted if someone else attempts to access your accounts.

However, bear in mind that this does not prevent certain agents, such as law enforcement or other state agents, from requesting your data from service providers. Many commercial service providers will hand over this data if requested. In your actor map, you may want to consider the relationship between those responsible for storing your sensitive data such as emails, your internet service provider and your government (if they are opposed to your work).

It might also be quite difficult for you to access your accounts if your phone does not have network connection or if you are travelling without roaming.

Marking your devices and checking for tampering

If you are worried that others may tamper with or access your devices such as your computer or phone, you may want to leave markings which are very difficult to replicate on certain parts such as your phone's SIM card and the cover protecting the hard-drive of your computer. For example, you can do this by writing on parts with UV-marker which can only be detected with a UV light, or nail varnish with glitter, which will leave a pattern near impossible to replicate. Check the markings regularly, especially after anyone else has, or may have had, access to your devices to ensure nothing has been tampered with.

Talking to a trusted and up to date IT specialist

If you are working as an individual, it's good to maintain a relationship with a trusted IT specialist who is keeping abreast of latest security issues and tools and can check your devices and ensure they are healthy. This doesn't necessarily have to be an expert, but ideally someone well informed and up-to-date. If you don't have access to an IT specialist, you can seek out local hackerspaces, IT hubs, maker spaces, "Crypto Parties" or online communities for help. However, try to reduce the extent to which you have to blindly trust anyone: reading resources such as Security in-a-Box and Me and My Shadow will give you a good grounding in the topic and help you to direct the conversation.

Improve your understanding of your devices and the information technology you use. Focus on those devices central to your work and security.

In an organisation, an internal IT specialist is useful. However, it's important that they are someone trustworthy who understands the kind of risks and threats which you face. If you have such a person at your disposal, they can carry out regular checks on the organisation's devices and guarantee their health, ensuring nothing is amiss and answering any questions you may have.

23 https://securityinabox.org/en/guide/avast/windows

24 https://securityinabox.org/en/guide/spybot/windows

Appendix C

Analysing Declared Threats

From the Front Line Defenders' Workbook on Security for Human Rights Defenders:

1. What exactly are the facts surrounding the declared threat?
   - Who communicated what, when and how?
   - If it was a phone call, were there background noises?
   - What was the language and tone?
   - Did it follow some (new?) activity of yours?

2. Has there been a pattern of declared threats over time?
   Patterns could include the following:
   - You receive a series of threatening calls or messages
   - You have been followed for two days and your son was followed yesterday
   - Another HRD was called for questioning by the authorities and then s/he was detained. Now you have been called for questioning.

   There could be patterns involving:
   - The type of threats issued
   - The means by which the threat is made (in person, by phone, etc.)
   - The timing of the threats (day of the week and time)
   - The perpetrators of the threats (if they are known)
   - The place the threats are made
   - The events preceding the threats, such as your organisation issuing a press release.

3. What seems to be the objective of the declared threat?
   - Is it clear from the threat what the perpetrator wants you to do? If this is not clear, sometimes the objective can be deduced from the timing of the threat. What actions are you planning or have you have taken recently?

4. Do you know who is making the declared threat?
   - Often you do not know. Do not jump to conclusions.
   - Be as specific as possible. If, for example, it is a police officer, which station is s/he from? What rank is s/he?
   - Consider whether a signed threat is really from the person/organisation whose name is used.
   - If you know who is making the threat, consider whether or not the perpetrator has the resources to carry out the threat.
   - If they have, that increases the likelihood that the perpetrator will follow up on the threat with an attack.

5. Finally, after analysing the above questions, do you think that the declared threat will be put into action?
   - This is a difficult assessment to make and you can never be 100% sure.
   - Your response will take into account your context including the history of attacks against HRDs in your country, the perpetrators' capacities, and the degree of impunity for perpetrators.
   - When in doubt, choose the option which seems to you to be the safest.

Appendix D | Exercises 3.1c and 3.2a

Identify New Capacities

Threat identified Consider to whom, by whom, how, and where.	**Capacities and existing practices**	**Vulnerabilities and gaps in existing practices**

New capacities required	**Strategy**		
	Acceptance	**Deterrence**	**Protection**

Appendix E

Security Wheel[25] for Evaluating Organisational Security Management

Evaluation
Problems: .....
Solutions: .....

Aquired security experience
Problems: .....
Solutions: .....

Response to indicators and incidents
Problems: .....
Solutions: .....

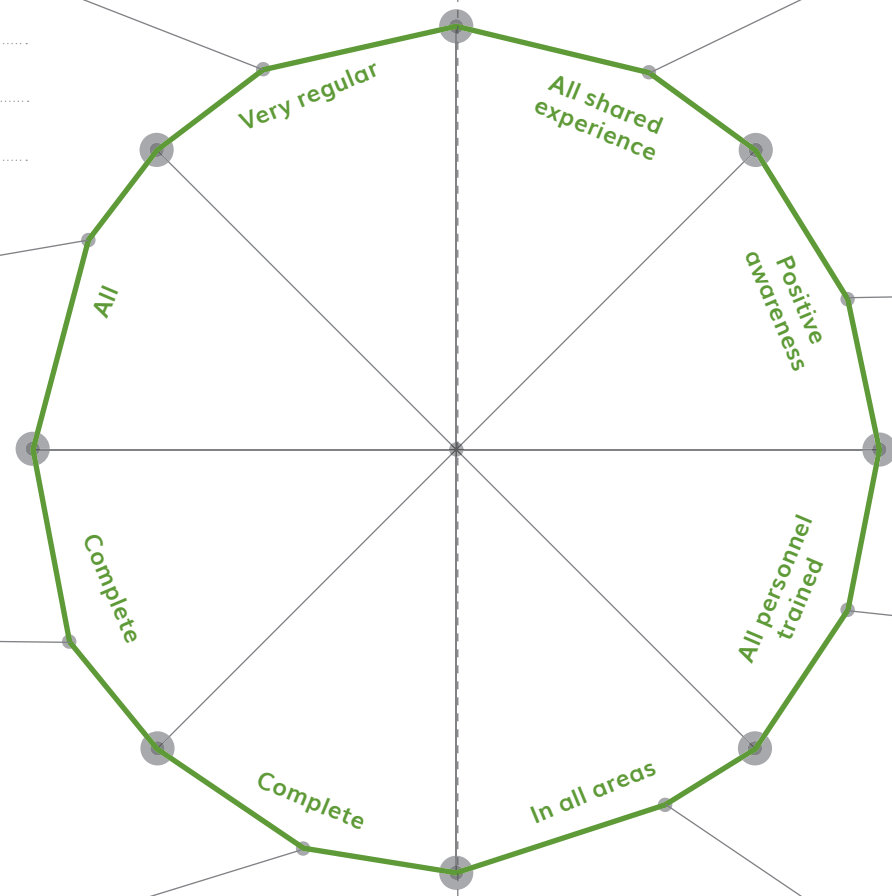
Attitude and awareness
Problems: .....
Solutions: .....

Ownership compliance
Problems: .....
Solutions: .....

Skills, knowledge, training
Problems: .....
Solutions: .....

Assignment of resonsibilites
Problems: .....
Solutions: .....

Security planning
Problems: .....
Solutions: .....



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

Appendix F

Do-No-Harm: Checking our Actions and Resource Transfers

Actions/resources	Impacts		
	Competition vs. inclusivity Questions to ask: ▸ Who is advantaged / disadvantaged? ▸ Could there be competition around this resource? ▸ How can we design our activities to be more inclusive?	**Substitution effects vs. appreciation and togetherness** Questions to ask: ▸ What existing practices are to be acknowledged and preserved/integrated? Or why shloud they be modified, abolished...? ▸ Who's responsibilities are positively or negatively affected by new measures?	**Selectivity and power relations** Questions to ask ▸ Is the resource linked to power? ▸ Will the resource add to someone's power? ▸ How can this be balanced or used constructively?
Example External security training for staff members	▸ non-beneficiaries feel set back ▸ competition who is allowed to travel? ▸ training = capacity building = better paid job opportunities ▸ competition between departments/ teams/members for money for training ▸ time competition between other activities and training	▸ staff member who was responsible for training others on security is reduced to a normal 'participant' ▸ time, which was previously used for other trainings or excursions is now used for security trainings.	▸ people trained, will feel/be seen as more important ▸ more knowledge = more power in the hierarchy

Appendix G

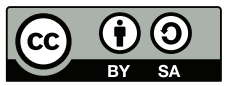
Do-No-Harm: Checking our Behaviour and Implicit Ethical Messages

	Messages and	possible impacts on/by	
Behavior/ Action	Yourself	Colleagues/Team	Opponents/ Adversaries
Changing all email communication to encrypted emails	**Message:** • I have something important to hide • I care for myself and my community **Impact:** ‣ Safer communication ‣ Burden of responsibility ‣ Increased paranoia or unfounded fears	**Message:** • If we don't encrypt, we don't have anything important • If I don't (manage to) encrypt, I don't care for myself or my community **Impact:** ‣ Feeling of shame ‣ Resistance to all security measures because of frustration encryption or time consumption...	**Message:** • S/He encrypts, therefore has something to hide • Only encrypted from certain moment on: Something important is happening soon • With whom is s/he exchanging encrypted emails? These are the most important contacts **Impact:** ‣ Danger of stronger digital and maybe physical surveillance for you and your community
Deciding for yourself not to work on weekends	**Message:** • I care for myself • Family is important **Impact:** ‣ Family is cared for ‣ Recharged energies ‣ Burnout prevented	**Message:** • S/He considers him/herself more important than our work • S/He is no longer able to work under pressure • Considers activism only to be a job **Impact:** ‣ Loss of trust ‣ Respect for self-care ‣ Jealousy ‣ Team spirit might suffer	**Impact:** ‣ Fewer activities on weekends ‣ Family is important, so family might be a good pressure point

	Messages and	possible impacts on/by	
Behavior/ Action	Yourself	Colleagues/Team	Opponents/ Adversaries
Organisational rule that human rights monitors always go in pairs on demonstrations/political rallies	**Message:** • Our work is risky (or has become riskier) • We are important to our organization **Impact:** ‣ Questioning: Is it too risky for me? ‣ Questioning: Is the organisation paranoid? ‣ Feeling valued	Same as individual	**Impact:** ‣ Stepping up monitor presence means more complaints etc. to come ‣ Needs more effort to deal with monitors

TACTICAL
TECHNOLOGY
COLLECTIVE

This manual was developed by the Tactical Technology Collective, a registered Dutch Stichting. For questions relating to the manual, or with regard to translating, distributing or re-using this content, please get in touch with us at ttc@tacticaltech.org.



Printed in Berlin, Germany by Oktoberdruck AG
Paper: Condat Matt Périgord
Typeface: Source Serif Pro, Muli

ISBN 978-3-00-053520-8

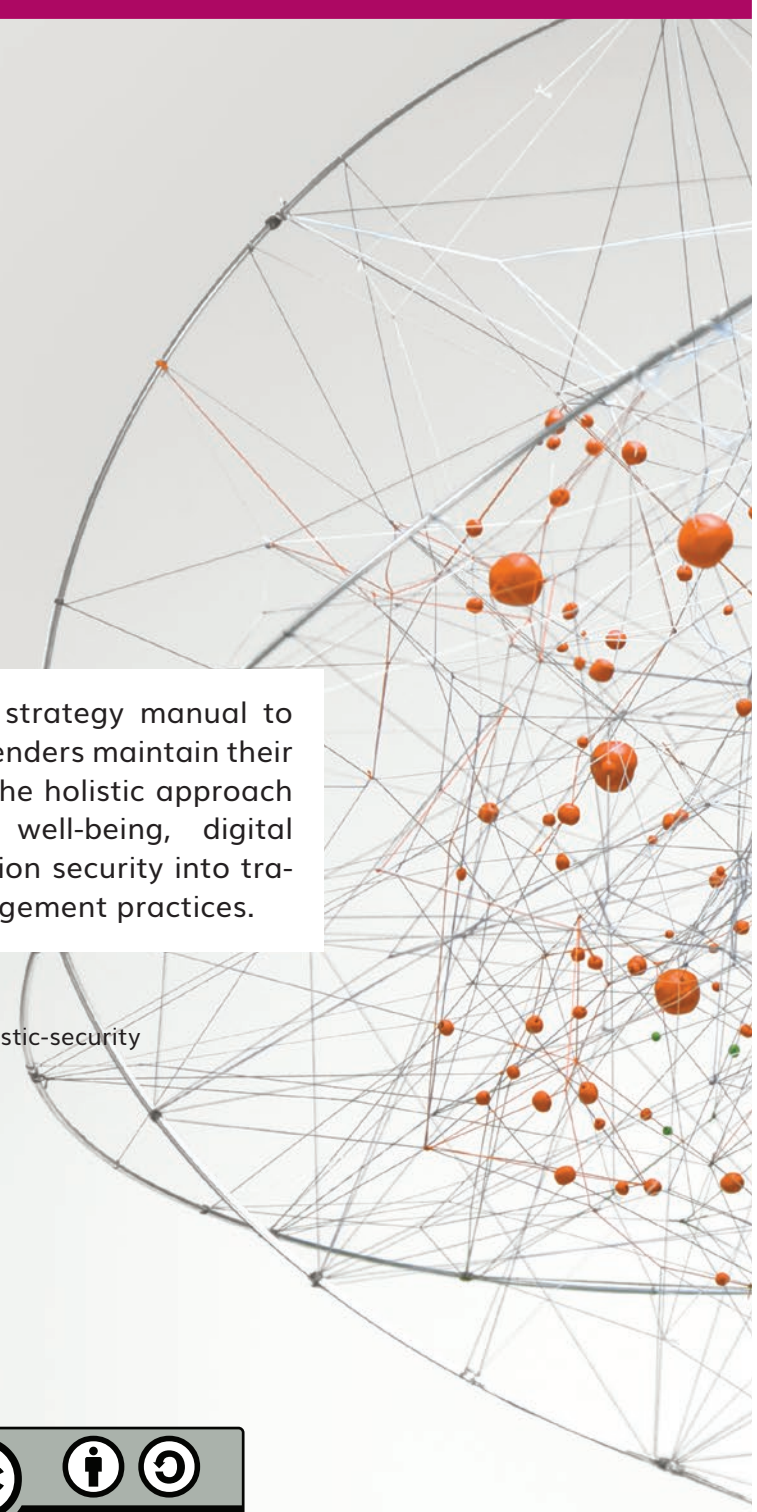
tacticaltech.org/holistic-security

Disclaimer

Holistic Security: a Strategy Manual for Human Rights Defenders has been written with the aim of providing human rights defenders with a selection of tested security strategies and tools chosen by practitioners in the field. Despite the fact that they have been chosen with the needs of this audience in mind, there is of course no 'one size fits all' solution. The legality, appropriateness and relevance of these strategies and tools will vary from one situation to another. In providing these strategies and tools, we advise you to select and implement them with a common sense approach. If you have any questions about appropriate use within your specific context or country, please seek the advice of a trusted local expert or request more information by emailing ttc@tacticaltech.org.

The strategies and tools referenced herein are provided "as is" without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. In no event shall the Tactical Technology Collective or any agent or representative thereof be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption), however caused under any theory of liability, arising in any way out of the use of or inability to make use of named software, even if advised of the possibility of such damage.

TACTICAL
TECHNOLOGY
COLLECTIVE



Holistic Security is a strategy manual to help human rights defenders maintain their **well-being in action**. The holistic approach integrates self-care, well-being, digital security, and information security into traditional security management practices.

https://tacticaltech.org/holistic-security

9 783000 535208

ISBN 978-3-00-053520-8