HOLISTIC SECURITY

Trainers' Manual

2016

TACTICAL TECHNOLOGY COLLECTIVE

Holistic Security is a project of Tactical Technology Collective. This publication has been produced with the assistance of the European Union with additional support from Free Press Unlimited. 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.

Table of Contents

Credits

Authors (except where otherwise indicated)

Craig Higson-Smith for Center for Victims of Torture
Sandra Ljubinkovic for Tactical Technology Collective
Daniel Ó Cluanaigh for Tactical Technology Collective
Ali Ravi for Front Line Defenders
Nora Rehmer for Protection International
Hannah Smith for Tactical Technology Collective
Bobby Soriano for Tactical Technology Collective
Peter Steudtner for Tactical Technology Collective

Based on the concept developed by
Craig Higson-Smith for Center for Victims of Torture
Daniel Ó Cluanaigh for Tactical Technology Collective
Ali Ravi for Front Line Defenders
Peter Steudtner for Tactical Technology Collective

Project Lead
Daniel Ó Cluanaigh

Coordinator
Hannah Smith

Additional writing by Hadi Al-Khatib, Mohammed Al-Maskati, Wojtek Bogusz, Rory Byrne, Adriana Dergam, Emilie De Wolf,Tessa Deryck, Jelena Djordjevic, Magdalena Freudenschuss, Ricardo Gonzalez, Alexandra Haché, Ronald Kakembo, Erick Monterrosas, Ginger Norwood, Fernanda Shirakawa, Sergei Smirnov, Tanya Spencer, Moritz Tenthoff, Pablo Zavala

Logo and illustrations
La Loma GbR

With special thanks to Neil Blazevic, C5, Enrique Eguren, Andrea Figari, Stephanie Hankey, Oktavía Jonsdottir, Azeenarh Mohammed, Anne Rimmer, Niels Ten Oever, Marek Tuszynski, Arjan Van der Waal, Chris Walker, Carol Waters

and our friends and colleagues from
Tactical Technology Collective
Center for Victims of Torture
Centre for Training and Networking in Nonviolent Action “Kurve Wustrow”
Front Line Defenders
Internews/Level-Up
Protection International.

Funders
European Union
Free Press Unlimited

About this Manual

This manual was created as a companion to Tactical Technology Collective's **Holistic Security - A Strategy Manual for Human Rights Defenders**. It was also created to reflect new knowledge and best practices identified through Tactical Tech's facilitation of dialogues and engagements between experts and facilitators in overall protection, digital security, and psycho-social well-being for human rights defenders (HRDs) between 2013 and 2015.

The **Trainer's Manual** is divided into three parts:

Part I includes general articles on best practices when facilitating security and protection trainings for HRDs, whatever their main focus may be (e.g. digital security, risk analysis, integrated security).

Part II includes 'stand-alone' sessions which are offered 'as-is' without explicit need for pre-requisites, and can be carried out in the context of any security-related training. They were designed by participants of the **Training of Advanced Security Trainers (TOAST)** event which took place in April 2015 as part of Tactical Tech's Holistic Security project. They were subsequently elaborated upon during a writing sprint in the same month.

Part III includes eleven sessions designed to form a sequential 'flow' based on the material from **Holistic Security: a Strategy Manual for Human Rights Defenders**. The sessions were developed for and tested at two four-day 'Introduction to Security' trainings held at the Centre for Training and Networking in Nonviolent Action "Kurve Wustrow" in 2015. They do not, however, represent the totality of potential sessions that could be created based on the manual. As such, we would encourage facilitators to take inspiration from the themes, approaches and ideas put forward here to develop and share further sessions designed to suit the needs of the groups they work with.

The structured learning sessions are largely organised according to the **ADIDS (Activity-Discussion-Input-Deepening-Synthesis) approach**,[1] an adult learning methodology that became popular among many of the authors through our work on the **Level-Up**[2] resource for digital security trainers in 2013 and 2014. We would like to extend our thanks to C5 for her inspiration in this regard.

We hope this manual proves useful to the community of facilitators and trainers who are responsible for processes of exploration and skill-building in well-being, security and protection of human rights defenders. We would like to extend our heartfelt thanks to the human rights defenders and practitioners from numerous organisations that have lent their minds, hands and hearts to this process.

1 For more about ADIDS, see https://www.level-up.cc/before-an-event/levelups-approach-to-adult-learning/#the-adids-approach

2 https://www.level-up.cc/

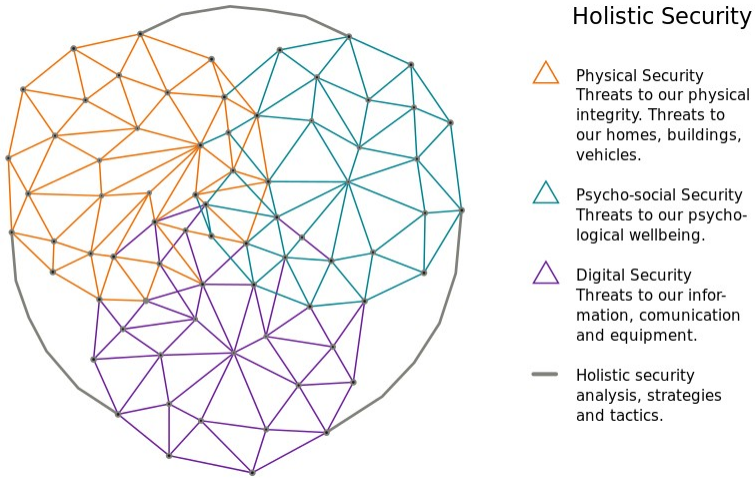
Part I

Best Practices

Walking the Talk: Facilitating Security Training from a Holistic Perspective[3]

Introduction

Holistic Security attempts to integrate best practices from – and mitigate differences between – different approaches to security and protection for human rights defenders (HRDs). It has focussed on at least three domains of knowledge which have developed in response to threats faced by HRDs. Many HRDs receive training and engage with self-learning materials focussed on these 'domains' of knowledge, including **digital security**, **risk analysis and security management** (also referred to as 'physical security'), and **psycho-social well-being** (sometimes called 'integrated security').



These three 'domains' have tended to be treated in relative (although not complete) isolation of one another, particularly when it comes to trainings. HRDs generally attend trainings that focus heavily on one domain and take little notice of other domains, in both organisation and content. This separation can have negative consequences. For example,

- a training on integrated security with HRDs at risk may be organised without due recognition that the participants are subjected to heavy surveillance, which may pose a threat to the training;
- a training on digital security may go awry if the facilitator teaches software tools without discussing the context in which the HRDs are operating;
- a risk analysis training may be challenged if no space is made to discuss the effect of stress on HRDs' abilities to accurately perceive and evaluate threats.

We believe that there are clear disadvantages to such approaches, which can endanger not only the learning process but may also threaten the security and well-being of facilitators and the communities they work with.

3 Based on inputs from the Tactical Tech “Holistic Security” Training of Advanced Security Trainers in Berlin, April 2015

However, the aim of the holistic security project is not for all facilitators to become experts in *every* domain of knowledge. Instead, the project aims to identify and fortify a **minimum level of knowledge and best practices in each domain** to avoid inadvertently endangering training events or participants through misinformation. Beyond that, it also works to foster collaboration among experts and facilitators in all domains in order to create approaches, frameworks and a shared language that is consistent and reinforces each domain of knowledge.

Adopting this approach as a facilitator means engaging with an iterative, critical and creative process of refining one's approach to facilitation. When working with individual HRDs and organisations, both individual and collective security-related experiences and needs offer many opportunities to become part of a wider process of change, both on a professional and personal level. However, being part of this process demands self-reflection from you as a facilitator about what role you can, ought and want to play in it.

Security as subjective and personal

Adopting a holistic approach to the security and well-being of HRDs means recognising that 'security' is—at its core—a deeply personal and subjective concept. The holistic approach begins by recognising that people define security and well-being for themselves, and they should be empowered to make their own informed reflections and decisions to foster and protect their integrity in the face of structural, armed, domestic and other forms of violence that try to limit the socio-political space for their work. In this context, HRDs define security for themselves, and we do not define it for them.

It follows therefore that there is no 'one-size-fits-all' approach to security. Security is to be defined and redefined in accordance with HRDs' own perceptions and ongoing analysis of the political, economic, social, technological, legal and environmental situations in which they operate, including threats to their well-being that may arise from their work. As facilitators of security and well-being capacity-building processes,, our task is not merely to offer 'security tools'. We also strive to foster and fortify HRDs' capacities for autonomous perception, analysis and the ability to respond to threats in an empowering manner consistent with their own definitions of security and well-being.

Context and risk analysis are therefore central tools in empowering HRDs to make informed decisions about their own security, and a number of frameworks and tools exist for facilitating this. In order to avoid fostering dependence and a potentially dangerous one-size-fits-all approach, all security-related training must pass on a minimum of tools and resources in order for HRDs to be able to continue learning and making informed security-related decisions beyond the training.

Capacity-building models that present risk or threat analysis as a clinical and objective process fall short of a holistic approach. Holistic security is anchored in the understanding that our sense of security is shaped by our emotional, spiritual and physical well-being. Therefore, only structuring trainings along supposedly rational and measurable lines of security management runs the risk of ignoring the individual, subjective and emotional realities that shape our perception of our safety and security needs. Our perception of the world around us is an unavoidable feature of our existence; it is the filter through which we understand and formulate any response to threats and dangers.

A further challenge to individual perception is the often secretive and increasingly pervasive electronic surveillance to which HRDs are subjected. Any security-related engagement with HRDs must recognise the potential or reality of this surveillance in both its content and organisation.

Our personal journeys inescapably inform our perceptions of the world. It is essential to acknowledge this reality when we consider and respond to threats. Our ability to accurately recognise and analyse threats is often challenged by factors including fear, stress, tiredness and trauma—experiences all too common among HRDs. Therefore, facilitating a holistic process with human rights defenders requires an implicit recognition of emotions as an integral part of any analysis and learning experience—for both participants and facilitators. This makes psycho-social well-being a crucial first step in facilitating critical reflection on security and well-being more broadly.

Creating a safe space

In organising and facilitating a security training for HRDs, we must bring with us a keen awareness of the context in which they are carrying out their work, the potential threats they may face (or experiences of threat they have survived) and the potential implications those threats have for the safety of the training itself, as well as in creating a healthy and productive learning experience for the participants.

As noted, evaluating and improving security is not an objective process, but rather one that hinges on our personal choices and perceptions. In order for it to happen most effectively, participants and facilitators must together create and maintain a safe space in which HRDs can reflect on their situations, engage in learning and capacity-building processes and make decisions in an empowered manner.

Creating a **safe space** for learning has implications on a logistical level, and also for the pedagogical approach we adopt. In this regard, no checklist is an adequate replacement for developing our own ability to assess threats to the training and participants, developing a keen sense for reading a group and responding to their needs. However, some generally useful resources, considerations and pedagogical best practices are highlighted here.

In short, a holistic approach to creating a safe space will recognise the following:

- People learn best when they feel safe, empowered and respected.
- Fear, stress, tiredness, trauma and other elements are factors that condition our learning experiences and ability to creatively work with our security. Many HRDs arrive at a training, bringing such experiences with them. At a minimum, facilitators must respect this reality, understand its impact on learning processes and how the event is organised, and avoid doing harm. This includes (but is not limited to):
    - choosing a location for the training where participants will not feel threatened
    - allowing dedicated time for HRDs to share emotional experiences
    - creating a space which is physically comfortable for participants
    - giving adequate warning and ensuring consent of participants before engaging with any potentially disturbing material or activities
    - respecting participants' autonomy to regulate their level of engagement with the content of the training
    - facilitating dialogue and building consensus on any of the above.
- Electronic surveillance is widely used against HRDs, and many HRDs will bring this reality

or their perception of it to any training relating to security and well-being. At a minimum, facilitators must respect this reality, understand its impact on learning processes and how the event is organised, and avoid doing harm. This includes (but is not limited to):

- understanding that content and metadata[4] of communications exchanged while organising a training may be monitored
- encouraging participants to communicate more securely and offering appropriate options where possible
- broaching the issue of device surveillance in an informed manner, without aiming to instil fear during participant agreements; establish a consensus with the group as to how best to deal with this issue during the training.

Gender and intersectionality

Threats and violence against HRDs are often the result of multiple discriminations. Aside from the fact that their human rights work may challenge powerful socio-political, economic and other interests, HRDs may be subjected to threats arising from their real or perceived gender identity, sexual orientation, race, ethnicity, language, migratory status (documented/undocumented), religion, socio-economic background or other factors. Acknowledging the systematic nature of how power structures lead to domination, discrimination and oppression is fundamental to counteracting them. This is relevant on a macro-level across the socio-political contexts in which we work, and at the micro-level of how they manifest inside the training space.

With this in mind, it is important for us as facilitators to be aware of the elements affecting our own position of power, and make space for acknowledging these structures within a training group. This approach is called **intersectionality**; it empowers us to deconstruct and challenge the influence of these factors both in our training and in the broader fight for human rights.

A intersectional, gender-conscious approach, combined with a thorough context analysis, can inform many of choices we make with regard to trainings. On a practical level this might affect the selection of facilitators, inform how they will approach the training and guide participant selection. With regard to content, it is vital that facilitators recognise that women and LGBTI HRDs in particular are subjected to additional gendered—and often sexualised—violence[5], both online and offline, as a result of their identity and work. Furthermore, they are often subjected to discrimination in terms of access to education and other resources (such as technology) that are relevant to their security. Facilitators must recognise and seek to address these issues.

Demystification and empowerment

Facilitators will almost always have a much stronger knowledge base in one 'domain' of security than in the others. No facilitator should claim or give the impression that they have expertise where they do not. However, basic knowledge is usually enough to demystify and highlight best practices from the other domains, and encourage participants to learn more from available resources (via self-learning or in-person trainings). While personal experience remains the best

4 Metadata or 'data about data', is information about digital transactions. For example, when an internet user sends an email, the 'metadata' generated and accessible to many will include their internet protocol address, the time and date, the recipient of the email, the services they use, and so on.

5 For more information on the distinction between gender-based and sexualised violence see link below: www.irinnews.org/feature/2004/09/01/definitions-sexual-and-gender-based-violence

guide for this, some important points that are always worth reiterating include:

- Self-care and well-being are not **selfish** but are rather **subversive** and **political** acts of self-preservation.
- Security measures should always correspond to context analysis and be in response to concretely identified threats.
- Digital data is a vital and often sensitive resource over which HRDs can and should take control. This is facilitated through access to autonomous, de-centralised platforms and free, open-source software.

'Facilitation' vs. 'training' – recognising the wisdom in the room

Although this manual is called a 'Trainers' Manual', you may have noticed that the term 'facilitator' is used much more frequently throughout the text. This is based on a qualitative distinction drawn between the terms 'facilitator' and 'trainer', wherein 'facilitator' is deliberately chosen to describe a more inclusive, open-ended, supportive, engaging role required by the holistic approach.

The aim is to encourage a shift away from the traditional perception of a 'trainer' coming to deliver wholly new knowledge and skills in a top-down approach. In contrast, as facilitators, our job is not to make decisions or rules for anyone. Rather, we are creating a space in which, through engaging with new knowledge, participants make their own decisions about security and how it is relevant to their activism.

This implies developing and maintaining awareness of the subjectivity of our own perceptions that are shaped by a multitude of internal and external factors. Thereby, we open a space for the existence of a multitude of truths and realities, which is important when we are defining a role for ourselves as a facilitator.

Human beings are natural security experts. Our evolution has been underpinned by the development of survival instincts and natural responses to threats and attacks, many of which are physiologically 'hard-wired'. The HRDs participating in a training may be operating in situations of great risk and stress. The fact that they have arrived at the training is testament to their ability to survive and credits the resources they have developed to this end.

When engaging with human rights defenders in a capacity-building process, emphasising and respecting existing coping strategies forms the basis of a mutual learning process. It is important that facilitators meet participants 'where they are' and understand and acknowledge their existing security practices (both good and bad). These can then be a vehicle for creative and critical reflection on the participants' security situation and practices, as well as a basis upon which new, improved practices can be built.

Co-facilitation, collaboration and longer term engagements

Co-facilitation among multiple facilitators with differing and complimentary areas of expertise has been identified as a best practice which offers participants an enriched learning experience, and better enables the facilitation team to cope with aspects of HRD security with which they are less comfortable or familiar. Furthermore, co-facilitation is a process that helps facilitators expand their skill-sets and knowledge of facilitation tools and techniques, as well as develop a shared common language across co-facilitators' respective domains of expertise.

Unfortunately, trainings (with or without co-facilitation) can be limited in their effectiveness by a 'box-ticking' approach, which treats the training as a one-off event within a discrete period of time, generally two to five days, with no funding for follow-up or accompaniment of a broader process of learning, whether within one 'domain' of security, or across domains.

Without building in a longer-term process of learning and increasing access to security and well-being resources, in our experience these one-off, isolated trainings are demanding at best and potentially harmful at worst. Follow-up after trainings, when carried out as an unfunded mandate, drains the resources and energy of facilitators and can lead to participants' needs for advice and resources being frustrated. Expectations of lasting change in security habits are seldom met by such trainings. Therefore, for more efficient use of resources and better outcomes, longer-term sustained engagements should be supported and one-off limited training engagements should not be encouraged.

Although not all organisations have a mandate or capacity to provide HRDs with access to security training from across domains, collaboration and networking should be encouraged in order to facilitate HRDs access to as holistic a process as possible. Community-building and learning among facilitators across domains is key to this process.

Walking the talk

Holistic security is not merely a theoretical approach to security management, but rather puts our subjective lived experiences as individuals and groups at its core. There is no simple formula or framework which can substitute experience. The first step in adopting a holistic approach to security training—regardless of our areas of expertise—is to begin to integrate this understanding of the subjective, personal and often emotional nature of our work into our own perspective as facilitators and/or activists. This is vital if we are to enable a process for HRDs to not only acquire the skills and knowledge necessary, but to also gain a self-actualized attitude and mindset towards building upon and improving their own healthy security practices.

Understanding the holistic approach requires us to look deeper into our own experiences, capacities, judgements, feelings, values, skills, personal histories, and develop an openness to evolving as trainers and facilitators. Looking inward is an important step toward feeling empowered to create conscious space for our emotional worlds in a training as a co-learning experience.

Engaging HRDs in a deeper conversation about the inter-connectedness of our emotions and security is only possible if we are open to diving deeper into ourselves, and understanding our own emotional realities. Drawing on these insights can help HRDs make decisions regarding their own security that are empowering and sustainable, since they are ultimately geared towards establishing, conserving, or restoring personal well-being and resilience.

The following resources endeavour to provide an opportunity for you as a facilitator to explore and reflect on your own experience and well-being as a continuous 'practice', before integrating new practices into your work with HRDs. Based on their collective experience, the authors encourage considering your own personal development as an iterative process, gradually moving forward with your own learning through the exploration, testing and integration of new techniques, strategies and best practices with regard to all aspects of your security and well-being.

What does this mean in practical terms? It may mean reflecting on your own emotional capacity to deal with various group processes. Ask yourself: Do I allow myself to feel and express various emotions? Do I ask myself how I feel? How does my work as and with HRDs affect me? As a result,

how do I treat my body, my partner, friends, relatives, and colleagues? Is my own well-being a priority in my life? Is thinking of my own well-being closely connected with feelings of guilt, especially when witnessing the bravery and struggles of HRDs I work with?

It may also mean looking at how you organise your approach to security: how you analyse your context, identify threats and make security plans, negotiate strategies, policies and tactics with your collective or organisation. Or if any of this takes place at all.

It may mean thinking for the first time about how you use digital information in your work: What sensitive information do you manage, store and communicate? What is the potential for its surveillance, and what should you learn in order to better protect your information, your self, your work and the HRDs you work with?

Having space to reflect on these questions may help you to connect more intensely with processes and dynamics within training groups and deepen your ability and confidence to productively deal with emotional conversations that come up during trainings and other interactions with HRDs. It also gives you the opportunity to explore the interconnectivity of your personal security across multiple domains, such as the integration of digital and other security tactics in your own life. We call this **walking the talk**. Living it, owning it, and understanding the inter-relatedness in the core of our being. And then moving on together with the activists and communities we work with.

Holistic Co-facilitation[6]

Working alone as a facilitator is extremely challenging and lamentably common. Dealing with the emotional nature of the training, difficult group dynamics, unforeseen challenges, receiving and processing feedback, and iteratively re-designing workshops while still trying to get enough food, fresh air and sleep are all extremely challenging when working alone. This becomes even more difficult when we set ourselves the goal of taking a 'holistic' approach to our workshops—a process that necessarily involves both internal self-reflection as well as engaging with new knowledge from different domains.

In the Introduction, we stressed the importance of our own well-being as facilitators. In this regard, co-facilitation—creating a team of two or more people to facilitate a learning process with a of HRDs—is an essential skill that can improve our well-being as well as expand our expertise and experience.

Trainer well-being

Working in a team as co-facilitators can be beneficial on many levels. It enables a sharing of responsibility and brings different individual strengths to the workshop or training. Having a colleague involved in the process provides support not only in the preparation of the training event, but also increases the opportunities for more ideas and different types of energy when dealing with tension or moments of conflict within the training group. The burden of workload and stress can, hopefully, be shared among co-facilitators. Lower stress levels among the facilitators then allow for far greater flexibility in approaches, increased reactivity to participant needs, as well as more space for 'lighter' and perhaps more humorous facilitation. In more technical trainings such as digital security trainings, it allows for better supervision of hands-on work and increases participants' access to assistance when they come across problems.

Working with a co-facilitator allows you to take a step back if you become too personally involved, and is hugely helpful when debriefing. It allows you to check your perceptions when reflecting on group dynamics, and makes the process of iteratively designing and re-designing workshops in accordance with participants' needs much easier. Most importantly, by working together you make facilitation less exhausting and intimidating. Debriefing about the emotional impact of facilitation and training is important, and is often much easier with a colleague who understands the context and has had a similar experience.

Building 'holistic' expertise

We strongly encourage co-facilitation across different domains and fields of expertise to deepen reflection and knowledge-sharing, as well as contribute to holistic approaches to security training. This potential is further enriched when you can collaborate with different genders, ethnicities, nationalities, ages, skills and knowledge domains, bringing intersectional perspectives to the group process.

Collaborating with another facilitator with distinct expertise can inspire us to create new

6 Based on inputs from participants at the Holistic Security Training of Advanced Security Trainers, Berlin, April 2015

approaches to training, help identify best practices and areas for improvement, and design new exercises. It also increases our freedom to be mindful of the emotional climate in the room, and be aware of the body language of participants (fidgeting,, yawning, sudden departures, etc.) and what it tells us about their engagement with the process. We have more space to observe facial expressions (if participants are engaged or completely absent-minded), and can look for patterns of communication and dynamics within various group processes.

It is often the case when focussing on a certain security domain during in a workshop—for example, digital security—that tangential questions will arise from the group about concepts that facilitator may not be familiar with, such as organisational security planning, or how stress affects us. Such issues will be much more easily addressed when co-facilitators can offer contrasting complimentary expertise. In general, participants will benefit greatly from having access to a much broader range of expertise during a workshop with multiple co-facilitators present.

Co-facilitation ideas and best practices

How to arrange co-facilitation depends greatly on the context of the event itself, and opportunities may be conditioned by factors including the length of the workshop, number of participants, funder priorities, etc. As with training in general, there is no 'one-size-fits-all' solution. However, there are a few best practices to keep in mind such as:

- **Have enough preparation time**: Working with someone new means working with new ideas, and this can make preparation a very inspiring, yet sometimes lengthy, process. Be sure to give yourselves enough time—perhaps a full day—to prepare together before the training.
- **Be open**: Working with someone from a different field of expertise can sometimes be challenging as they may have a different perspective on security. The process will work best if both sides are open to developing new perspectives, rather than simply defending their own.
- **Be consistent**: Building a holistic approach to training is not as simple as simply taking turns training on our own material: there are sometimes implicit contradictions in our discourses which can mean we undermine each other. For example, a digital security facilitator may find her day's work of awareness-raising undone by a legal expert co-facilitator who begins their session with "I, by contrast, have nothing to hide!"
- **Build examples together**: Demonstrative examples from real life are often very useful learning tools. It's a great idea if facilitators can use the same examples to tease out different aspects of security from the same scenarios. Participants themselves may be a great source of such scenarios.

Different workshops can have very different structures, and this can impact on the kind of co-facilitation possible, and depending on the relative expertise of the facilitators involved. Some potential formats for collaboration could include:

- **Cross-training**: Here, one facilitator acts as a participant in the training, in order to learn the skills themselves. This way they can give very refined, participant-perspective feedback to their colleague in the debriefing.
- **Trainee-swap**: A 'trainee swap' for a period of time during the workshop for participants to have access to the fundamentals from each domain. Two workshops on 'separate' security

topics can be arranged simultaneously.

- **Informal evening sessions**: It can be particularly helpful for an optional informal evening space to be set up for participants to 'deep dive' on additional skills and knowledge. Digital security 'hacklabs' are one such possibility, and similar spaces can also be set up for psycho-social support, or risk management and security planning help.

Checklist: Creating a Safe Space[7]

As discussed in the chapter **Walking the Talk**, creating a safe space is a vital part of holistic security training and better enables HRDs to reflect on their situation, engage in learning and capacity building processes, and take decisions in an empowered manner. To achieve this, an awareness of the context in which HRDs are carrying out their work, the potential or actual threats they face, and their experience as survivors is vital. We must also take care to assess the potential implications of such threats for the safety of the training itself, as well as for creating an optimal and productive learning experience for the participants.

Creating a 'safe space' for learning has implications on a logistical level, and also in terms of the pedagogical approach we adopt. Some generally useful guidelines are noted in the non-exhaustive checklist below.

Preparation

Communication

Naming the event: In some cases, it is a good idea to be open about the nature and other details of an event, especially if it is supported or sponsored by a respected organisation that can offer some protection to participants with the weight of its reputation. In other cases, however, it is best to avoid 'naming' the event too accurately (for example, a sign in the hotel stating 'Digital Security Training for LGBTI Activists'). Consider whether you even need to share the exact nature of the event with the venue.

Local source of information: If you are training in an area with which you're unfamiliar, it is advantageous to have a local partner help with the security analysis of the training to ensure you can make informed decisions based on accurate information.

Channels: If possible, use a secure means of communicating with organisers or participants before the training. Add this as an agenda item from your first contact. Although establishing secure communication channels immediately is not always possible, it's important to at least be aware of what insecure communication options may reveal.

Safe travel and emergency numbers: ensure that you and participants are aware of the safest way to arrive at the training venue and have the emergency services' numbers in the country or region.

Travel and Logistics

Participant selection: Consider the **Do-No-Harm Principle**[8] when selecting participants. Often, trainings constitute an intervention in a situation of multiple conflicts (between HRDs and their adversaries, but also among HRDs along gender and other lines of potential discrimination). Ensure that the training doesn't aggravate such conflicts. In some cases, this may mean limiting participants to one group, whereas in other cases, it is best for all groups to be represented, with time dedicated to raising awareness of and countering the dynamics of privilege that may exist

7 Compiled from an exercise carried out at the Holistic Security Training of Advanced Security Trainers (Tactical Technology Collective), Berlin, April 2015.

8 For further information, see the chapter *Security and the Do-No-Harm Approach* in the *Holistic Security Manual:* https://holistic-security.tacticaltech.org/chapters/strategise/3-6-security-and-the-do-no-harm-approach

within the group.

Safe travel: It's possible that participants from the same organisation, region or country travelling together on the same flight to the same location at the same time might attract the unwanted attention of the authorities. If you are unsure of the potential risk, consult with participants or look for precedents. Consider having participants take different routes and flights. If it is safer for participants to travel together, prepare for potential reprisals when participants re-enter their region or country of origin.

Read the local news and weather: Before travelling, it's good to get a sense of the local political context and developments, as well as weather and other environmental factors which may affect the training.

Characteristics of the training location

Note: There is no perfectly 'safe space' for a training any more than such spaces exist elsewhere in the lives of most HRDs. You will invariably have to make compromises on some of the items below. The best practice in this regard is to simply be open and honest with participants about the decisions that were made and the reasons for them, and to make decisions as a group (if possible) about how to mitigate the effects of any of these compromises.

Natural light and nature: Venues with access to natural light sources and green spaces such as parks, forests or gardens greatly support learning and relaxation.

Proximity to health facilities, pharmacies and healers: It is not uncommon for participants to develop minor illnesses during a training, or suffer from physical discomfort following extended periods of stress. It is a good idea to consider a venue with access to a pharmacy, other health facilities, counselling or 'alternative' therapies.

Different bodies: The space should ideally be wheelchair-accessible, and considerate of participants who may suffer from reduced mobility or other physical challenges.

Historical significance: If possible, try to find out something about the history of the space, especially in areas affected by conflict. Consider the political role (if any) of the owner of the space. Locations preferred by NGOs or owned by NGOs are advantageous.

Size: More space to move, think and work in different combinations is an advantage.

Room layout: In some cultures, people physically separate themselves in a shared space according to strata of privilege (for example, men at the front, women at the back). Try to immediately disrupt this if necessary, in order to challenge dynamics of dominance and privilege.

Food: Access to good, healthy food is vital for the learning process. Consider participants' diets or allergies (vegetarian, vegan, kosher, halal, coeliac/gluten-intollerant) and opt for healthy foods as snacks. If possible, buy from local producers.

Surveillance: Security cameras are increasingly common in public spaces. If they are present in the training space, speak to participants about this. Consider requesting that the venue switch them off.

Connectivity: Internet access is important for many trainings, but be aware that in hotels and other public spaces its use may be monitored, and share this information with participants.

Other guests: Consider whether the space will be used by several groups at once. Who will these other groups be, and what is their relationship to the participants?

During the training

Noting vulnerabilities: There is no perfectly safe space for a training. To the extent you are aware of them, it is a good idea to share the security vulnerabilities of the space with participants to establish awareness and agree on some security measures to maintain the safety of the space.

Language: Where possible, facilitators should speak the same language as the participants. If this is not an option, or in mixed language groups, employ translators or recruit volunteers from the group so that those who don't speak the main language of the training well can still access the knowledge and feel included. Encourage language groups to work together when necessary, but try not to cut them off from the rest of the group.

Ground rules/agreements: Always establish shared agreements early in the training, which serve to foster and maintain the safety of the space. In the process of defining a shared agreement with participants, consider the following:

- **Anonymity**: Participants shouldn't be forced to share their real names or any other details if a threat of infiltration exists.
- **Confidentiality**: Establish clear protocols for recording and sharing of data. No participant should be forced to have anything they say or even their presence at the event shared by another participant without their permission. In this regard, social media usage should be spoken about.
- **Step up, step back**: This concept is used to encourage quieter participants to 'step up' and contribute more in group situations, and for participants who tend to speak more than others to 'step back' and allow space for others to contribute. This also presents an opportunity acknowledge intersectionality (p. 9) and counter the dynamics of structural privilege which may, for example, lead to certain individuals or sub-groups not voicing their opinions, or to others dominating.
- **Electronic devices**: While access to electronic devices may be very important for participants who wish to follow developments at home or keep in touch with friends and relatives, the potential for surveillance should be flagged and agreements should be established about when and where it is acceptable to store and use devices.
- **Sharing security indicators**: If any participant or facilitator notes anything out of the ordinary which may indicate a change in the security situation of the training, they should report it to the facilitator and analyse it together. The facilitator can decide whether it should be shared with the group or not.
- **No discrimination**: It should be stated outright that no discrimination, sexism, homophobia, transphobia or racism will be tolerated in the group.
- **Access to the space**: Establish who is allowed into the training space and the preferred protocol for anyone else being allowed to join should the situation arise.

Have a Plan B: If possible, it is a great idea to have an alternative location for the training, in case anything goes wrong and the original location can no longer be used.

Check-ins: Begin each day by 'checking in' with participants on anything happening outside of the training, how they are feeling generally and whatever may be on their minds (such as events happening in their home region or country). Also give participants space to share any security indicators they have noticed in the immediate surroundings of the event.

Documentation: Ensure that any sensitive information on paper, flipcharts or other formats is tidied up and safely stored or disposed of at the end of each day.

Follow-up

Manage expectations: Do not create expectations among participants that you will be able to dedicate more time to follow-up than is realistic for you. The most important thing is to be honest and to try to offer alternative resources if your energies and time are limited. If possible, identify a local 'champion' in advance who could be a potential resource for the community.

Secure communication: Try to establish a secure means of communication for participants after the event. Avoid centralised social networking platforms such as Facebook or Google Groups unless you are convinced that they will not be placed under surveillance. Alternatives such as **we.riseup.net** [9] or **diaspora*** [10] are less likely to collaborate with authorities. However, they can also be 'red flags' for people conducting surveillance because they are associated with activism and used less than corporate platforms.

Regular communication: Establish a rhythm for checking in with participants after an event in order to maintain and encourage contact.

9 https://we.riseup.net/
10 https://diasporafoundation.org/

Emotions and Learning[11]

One of the most important developments in the holistic approach to security training for HRDs is recognition of the role that emotions play in the learning process, and how this can impact both our facilitation style and our personal lives. While emotions are an important conditioning factor in any learning process, they are particularly relevant in trainings for HRDs.

There are a number of reasons for this. The threats, stress and fatigue experienced by HRDs make the concept of 'security' inherently very emotionally powerful. Security trainings, therefore, can often create a space where HRDs process and sometimes share the emotional nature of the issues facing them. Dealing with this natural process respectfully and tactfully is important for achieving the objectives of your workshop, for the well-being of the participants, and for your own well-being as a facilitator. However, as we will explore below, it is hard to identify 'hard and fast' rules for how to deal with emotions in the training room, and the best tool available to you is a keen awareness of your own emotional experience and a sensitivity to that of others.

Emotions and training HRDs

Emotions are a subject of ongoing scientific debate, but there is a consensus that there are at least six basic emotions that every human being experiences irrespective of cultural differences: happiness, sadness, surprise, fear, disgust and anger. The word emotion includes 'motion', as in 'movement'; emotions have a tendency in a particular direction, sometimes as a result of human evolution. They affect not only your feelings and thoughts, but also your body, which can in turn suffer and impact your emotions.

While we all have these six basic emotions, a number of secondary emotions are related to each of them. These secondary emotions and the ways in which we express them can differ greatly according to many factors, including our socio-cultural context. As facilitators, we carry our own socio-cultural interpretations of emotion with us, and may use our own conceptualisation of emotions and appropriate responses to them in the context of our participants.

> "I went to meet some HRDs working in an area occupied by an extremist group. In the meeting, I was asking one of the HRDs about technology, I was asking about his computers, his devices and so on. Then he started crying because he remembered what happened to him: how he was forced to leave his house and it was demolished. He had lost so many memories, and had wanted to give the house to his family. In that moment, I didn't know how to deal with it – I came to them to talk about digital security, and they gave me a lot of feedback on emotional things that had happened to them. I was shocked, so I decided, I will not talk about digital security for now. I stopped the presentation: you can't continue and say okay, let's talk about viruses and malware…"
>
> Trainer, Middle East & North Africa

When we consider our own security and well-being, thinking about our family and community can easily become an emotional activity. HRDs are no exception to this, may be more susceptible

11 Edited by Daniel Ó Cluanaigh for Tactical Tech. Adapted from a talk by A. Dergam and P. Steudtner at the *Holistic Security Training for Advanced Trainers*, Berlin. Also contains material reproduced from C. Higson-Smith/Center for Victims of Torture, "The Psychological Underpinnings of Security Training", https://www.level-up.cc/resources-for-trainers/holistic/psych-underpinnings/

to it if they may suffer from very serious threats, or have been subjected to violations of their human rights.

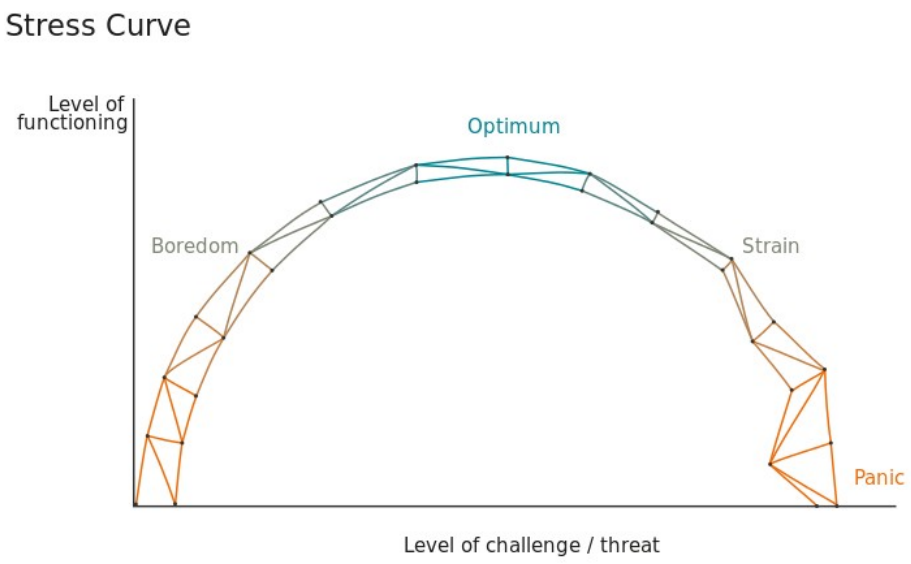
It is very natural for the emotional nature of security to make itself felt during a training. Emotions can be easily stirred by opening the space to consider the threats HRDs face, or through learning about threats or vulnerabilities of which participants were previously unaware - as is common when learning about digital security. These emotions can be expressed in many ways, and this can vary greatly depending on a number of socio-cultural factors. While some participants may speak openly about their feelings and experiences, perhaps being overtly angry or sad, others may express their feelings in more subtle ways which we also need to be attuned to. In any case, emotions are fundamental to the learning experience of participants and, as facilitators, we cannot ignore them.

How emotions affect learning

Good trainings are an exercise for participants in leaving their **comfort zone**. Consider some of the moments where you have learned most in your life: many of them will have also been moments of drama, difficulty, excitement, or humour. A good training may include all of these.

It may be useful to imagine participant comfort and discomfort as a curve having three 'zones':

1. **The comfort zone**: Participants are completely comfortable; they are not challenged or stressed. As a result, they tend not to learn because there is nothing to learn about! Rather, they feel relaxed in a situation that they find agreeable and do not feel the need to change.
2. **Productive stress**: Participants are challenged by new ideas and knowledge. The content may include information about threats, new technologies, and concepts that participants have to find ways to apply in their work. Participants can relate this new knowledge to their work and personal lives. In this zone they are able to actively learn.
3. **The alarm zone**: The content of the training 'crosses a line' to a point where participants are overwhelmed and do not feel empowered. They may become scared, disappointed or frustrated. Previous traumatic experiences may be aggravated, causing participants to 'close down' and stop learning.



Our approach as facilitators is to try to bring participants from the 'comfort zone' into the 'productive stress' zone for optimal learning. This is something many facilitators will have a feel for. Adult learners – being internally motivated and self-directed – are often happy to engage with this as participants. However, problems may arise when we overstep the 'productive stress zone' and participants begin to enter the 'alarm zone' towards strain or panic. At this point, our role is to facilitate a way back to the 'productive stress' or 'comfort' zones.

Fear, stress and fatigue

When gripped by fear, the human brain acts to protect itself without the need for conscious thought. This is a survival instinct developed over hundreds of thousands of years of evolution. While it is extremely effective at keeping us alive, it is not conducive to learning. When we are consumed by fear, our brain is not concerned with learning, but rather, with survival.

Fear can often show up in security-related trainings. For example, if a training takes place in a dangerous location or under dangerous conditions, participants may remain in 'survival mode' and not be able to effectively learn. Furthermore, even in a safe setting, if a facilitator recklessly uses fear as a tactic to demonstrate threats or vulnerabilities, this may make effective learning all but impossible. Depending on how they are implemented, common examples of using fear ineffectively include certain kinds of role play, exploiting network vulnerabilities or breaking into online accounts without adequately briefing and obtaining the consent of the participant involved.

Just as hosting a training in places where participants feel unsafe and stressed can make effective learning a challenge, removing participants from familiar contexts can create other challenges. Many HRDs suffer from extremely high levels of stress not only from threats they face, but also from huge the workloads they often have. Some facilitators will also be able to relate to this challenge! A training (on security or any other topic) that takes place outside of HRDs context may be the first opportunity in a long time for participants to 'switch off' while they experience a new place, new people and relative luxury. As a result, they may relax and as they do so, the effects of prolonged stress can make themselves felt. Many participants may be fatigued and simply need to sleep, while others will have nightmares and discomfort. Some may find themselves boundlessly energetic and enthusiastic to be in new surroundings, while others may fall ill. All of these processes are natural and have little or nothing to do with you as a facilitator, your approach or indeed the content, but it is useful to keep in mind that trainings do not happen in a vacuum.

Best practices

The above issues can be intimidating for facilitators who often feel a sense of responsibility and a need to **control** what happens in their workshops. The universe of human emotions and the ways in which they are triggered and expressed is simply beyond our control. Nevertheless, a number of best practices can help us to recognise and respect the emotions present during the workshop. These practices are best created, refined and adapted by maintaining a keen awareness of your *own* emotional state.

Create an explicit space for people to talk about how they are feeling about what is important to them. This can be as simple as an open ('popcorn-style') go-around with the group at the beginning of each day. You may ask if there is anything **beyond the content of the training that they would like to talk about (for example, about anything back in their home towns, cities or countries).** You can also create these spaces according to your own reading of the group's energy. Participants will generally appreciate this check-in, and in most cases nothing too challenging will come up.

However, if a more emotional story is shared:

DO	DO NOT
• Remind people that they can say as much or as little as they like. • Listen respectfully. • Ask about what happened, what they did, and what they learned. • Monitor body language, tone of voice, and facial expressions for signs of increasing anxiety. • Help people finish their story, even if it means skipping over the most upsetting parts. • Thank people for sharing difficult experiences. • Give distressed people space to recover their composure by moving on to other topics and distracting the group. • Follow up with distressed people privately to see if they would like further support. • If they are crying, ask if there is anything you can do to make them more comfortable.	• Dismiss, minimize, or reject any part of the experience. • Pressure people into talking about their fears or past distressing experiences. • Ask people to close their eyes and imagine bad things. • Ask probing questions, especially those relating to feelings and thoughts. • Blame people for what happened to them. • Offer meaningless platitudes such as “You were so lucky to survive, it could have been worse!”, “I know how you feel!”, and “It will be alright!” None of these are in fact true, and all are potentially insulting. • Offer unsolicited advice, suggest counselling, or label a person’s mental state in public. • Over-react to their distress, and in so doing, make it worse. • Awkwardly pass tissues to someone who is crying: this can give the message that crying is wrong and that they should “pull themselves together.” • Assume that they do, or don't want to be touched or comforted.

We must also consider how to manage our own energy and ability to continue listening. In informal spaces in the evenings, participants may begin to open up and tell stories about their experiences. Participants may share information about themselves, or in other cases we may seek to find out more about their experiences (such as past security incidents) for our own information.

Especially if it seems like there is a lot they want to discuss, it's a good practice to reflect inwardly before entering the conversation: **How much time (in minutes) can I listen?** Make up your mind about this and **be clear and honest with them about how much time you can give to the conversation**. This way, you can give them your full attention without worrying about time. They will be better able to regulate what they share with you, and it will also facilitate your ability to bring the conversation to a close.

In the end, there is always a time limit. Some things must get left unsaid, and it's important that you are able to wrap up and 'land' properly from a sharing session. This can feel aggressive or calculated, but it's better to be able to exit gently rather than suddenly.

Traumatic stress reactions

We may have participants in our trainings who have suffered from traumatic experiences. It is often the case that trainings are scheduled not long after some kind of attack or accident, which spurs the individual, group or organisation to think about security. In these cases, it may be that some or all participants are recovering from a life-threatening event. A healthy response to traumatic events of this kind is characterised by symptoms such as light sleeping, being easily startled or angered, avoidance of anything associated with the event, and constant thinking about and analysis of the event. These symptoms normally last for four to six weeks after an incident. Considering these realities, organisers should carefully consider whether a training (especially a more technical or conceptual training) is a good idea within this time frame as it is unlikely that there will be much space for participants to learn new skills.

In general, past traumatic experiences do not necessarily pose a challenge to learning. For the most part, participants will respond perfectly well to the same 'productive stress' that anyone else finds useful to learn. In fact, survivors of traumatic events often grow significantly as a result of their experiences and may be very adept at creating, maintaining and updating healthy security and well-being practices.

However, for some people the normal process of recovering from a life-threatening experience fails, and they experience unhealthy traumatic stress reactions as a result.

Trauma related disorders[12]

- **Acute Stress Disorder (ASD)** is characterised by extreme anxiety, distress, and dissociation in the weeks immediately following a life-threatening event. People suffering ASD often report feeling strange, dreamy, or as though they are not quite in their bodies (depersonalization), and may not be able to remember parts of the traumatic experience.
- **Post-Traumatic Stress Disorder (PTSD)** is characterised by lasting intrusive memories, thoughts, and images of the life-threatening event, avoidance of reminders of the event, avoidance of thinking about or remembering the event, as well as feeling unsafe and anxious.
- **Complex Post-Traumatic Stress Disorder** is characterised by lasting emotional dis-regulation such as persistent sadness or explosive anger; dissociative episodes similar to those described under ASD; feelings of intense shame and guilt; being preoccupied with the perpetrator or preoccupied with revenge; and a loss of trust in other human beings. **Note:** Complex PTSD is not yet formally recognized as a psychiatric disorder.
- **Traumatic Bereavement / Prolonged Grief Disorder** is associated with the sudden and violent death of a loved one and is characterized by continuous sadness and unameliorated yearning for the deceased more than a year after their death.
- **Trauma-Related Depression** is characterized by severe and persistent sadness, crying, social withdrawal, fatigue, and loss of energy following a life-threatening event.
- **Trauma-Related Substance Abuse** involves the unhealthy use of alcohol, marijuana, amphetamines, sleeping pills, and over-the-counter medications. These drugs may initially be used as a way of coping with the symptoms of PTSD or other trauma-related conditions.

12 From C. Higson-Smith/Center for Victims of Torture, “The Psychological Underpinnings of Security Training”, https://www.level-up.cc/before-an-event/psychosocial-underpinnings-of-security-training/

If someone suffering from any of these conditions, it is usually inappropriate for them to participate in a security workshop focussed on anything other than their psychological well-being. It is not the role of security facilitators to diagnose emotional or psychiatric conditions. However, it **is** helpful to be able to recognize when a traumatic reaction is no longer healthy or adaptive. If you have a participant in your training who you feel may be suffering from an unhealthy traumatic stress reaction, consider the following do's and don'ts.

DO – *IN THE CLASSROOM*

- Limit the person's exposure to stories, images, and conversations that are upsetting to them.
- Help the person to stay present by offering healthy distractions and physical activities.
- Reassure the person that he or she is currently physically safe.
- Reassure the person that he or she can choose how they wish to participate in the training (or if they'd would rather not participate).
- Protect the person's privacy and dignity. Do not 'single them out' in front of other participants in the classroom while attempting to support them.
- Stop others from invading the person's privacy.

DO – *IN PRIVATE*

- Provide them with basic information about traumatic stress as described in this module.
- Respectfully and gently suggest that they seek professional assistance.
- Provide them with links to good mental health information online.
- Put them in touch with a local mental health professional with experience in traumatic stress.
- Follow up with them privately to see if they would like further support.

DO NOT – *AT ANY TIME*

- Ask probing questions about their traumatic experiences.
- Ask questions about their emotional health, either historically or in the present.
- Offer meaningless platitudes.
- Offer any kind of mental health advice or diagnosis.
- Suggest any medication, even homoeopathic.
- Over-react to their distress and in so doing make it worse.

Part II

Stand-Alone Sessions

Contents

Introduction

The 'stand-alone' sessions which are set out in this section can be carried out in the context of any security-related training without specific pre-requisites. They were designed during the development of *Holistic Security: a Manual for Human Rights Defenders* by participants of Tactical Tech's **Training of Advanced Security Trainers (TOAST)** which was held in Berlin in April 2015. The event brought together 25 trainers, facilitators and human rights defenders from around the world to share their experiences and develop best practices by pooling expertise and front-line experience from a range of disciplines, including digital security, psycho-social well-being and physical security.

Each of the sessions uses a central theme to help participants begin to think about their security in a holistic manner, drawing out the interlinkages between different aspects of their security, and providing a basis upon which facilitators can then focus in on key elements for more in-depth or technical sessions later in the training.

All the structured learning sessions in this manual are organised according to the **ADIDS (Activity-Discussion-Input-Deepening-Synthesis) approach**,[13] an adult learning methodology that became popular among many of the authors through our work on the **Level-Up**[14] resource for digital security trainers in 2013 and 2014. The ADIDS approach plays on the many different ways in which adults learn, allows participants to take an active role in their learning, to contextualise for themselves what is being learnt and why, and to better internalise new content. Each session guide also details the **knowledge**, **attitudes** and **skills** which comprise the major learning outcomes for the session.

Activity usually comes at the beginning of a session to introduce the topic in an interactive way and highlight key issues that can be drawn out in the rest of the session.

Discussion allows participants to talk and think more in depth about the topic. You should be prepared to help guide the discussion with key questions or discussion points.

Input usually takes place lecture-style, where the facilitator provides more in-depth, detailed information on the topic, expanding on concepts and themes which have been touched upon earlier in the session.

Deepening participants get to try out and apply the theory that they have learned in the earlier parts of the session in a more hands-on way.

Synthesis provides an opportunity to summarise the session and return to any unanswered questions which may have come up for participants during the session.

13 For more about ADIDS, see https://www.level-up.cc/before-an-event/levelups-approach-to-adult-learning/#the-adids-approach

14 See https://www.level-up.cc/

Introducing Holistic Security

This is proposed as the first session for trainings that seek to provide a holistic view on security and include dimensions of physical, psycho-social and digital security in their risk analysis. The session plan constitutes a scene setter/grounding exercise at the beginning of a training (possibly followed by collecting expectations, making agreements etc.)

Objectives & Requirements

Attitudes: Active recognition of the subjectivity and emotional dimensions of security; awareness and inclination to act on security ('taking it seriously').

Knowledge: Understanding the way in which different aspects of our security are interlinked.

Skills:: Ability to identify different elements (digital, physical, and psycho-social) which impact upon security in a practical scenario.

Prerequisites: None

No. of Facilitators: 1

Technical Requirements: Sheets of paper with the scenario printed on it (or a projector to display the scenario), flipchart/whiteboard, markers.

Theoretical and Online Resources: Holistic Security: a Manual for Human Rights Defenders (https://tacticaltech.org/holistic-security)

Time: 60 minutes (120 minutes with optional exercise)

Contributors: Adriana Dergam, Daniel Ó Cluanaigh, Nora Rehmer, Sergey Smirnov

Activity & Discussion (20 minutes)

Step 1. Participants are given time to read the following scenario either printed out or projected via a screen.

> Olga Alekseevna [can change name] is a human rights defender travelling to attend a conference abroad. She is going to present a report on the situation of human rights in her country. She is travelling with some equipment including her mobile phone, computer and USB flash drive, which contains some drafts of her report. She hopes to finish the draft once she arrives. She is travelling alone, and when she goes to the airport and arrives at customs, officials who do not identify themselves approach her. They ask her directly whether she has any 'digital devices' with her. She is surprised and nervous and since she does not understand what 'digital devices' means, she answers *"No"*. The officials then ask her to put her bag through an x-ray scanner, and discover the USB flash drive in her bag. She is then asked to take the flash drive from her bag and hand it over to them. Olga thinks about challenging them and telling them they have no right to take her device, however she is not sure in this case what her rights are, and she is also afraid that if she argues with them, she may miss her flight and not have the chance to present her report. They ask her to wait, and they disappear into an office for fifteen minutes with her flash drive. When the officials return, they hand back her the flash drive, and wish her a pleasant flight. She is

nervous throughout the flight, worrying about what has happened to her flash drive and the data that was on it. When she arrives at her destination, she turns to her colleagues for advice.

Step 2. Invite participants to reflect on the scenario and capture key elements of the discussion on a flipchart. The following questions may be used to initiate deeper reflection on certain aspects:

- What did you observe in this scenario?
- How do you think Olga felt when the security agents approached her?
- Would she have felt differently if somebody had been with her?
- What valuable assets did she have to protect (e.g. the value of the information on the USB stick)?
- What devices/media did she have (e.g., computer, cell phone, USB stick)?
- What is the legal background of this story? How could she have reacted had she known her rights in this situation? Did she have rights to claim her USB stick back or not to give it away at all? (Consider asking participants if they are aware of the legal regulations in their own country.)
- Who could be her allies? Whom could she have contacted in this situation?
- What could have happened to the USB drive while it was in the hands of the officials?
- What might the consequences be of security officials taking the USB stick away, even for a short time, for Olga or others?
- What was the role of Olga's organisation in this situation? Did they analyse the risks of the journey? Were they supportive?
- Would she have been as nervous or would she have behaved differently of they had discussed and rehearsed this situation at her organisation beforehand (mental rehearsal, role play, etc.)?

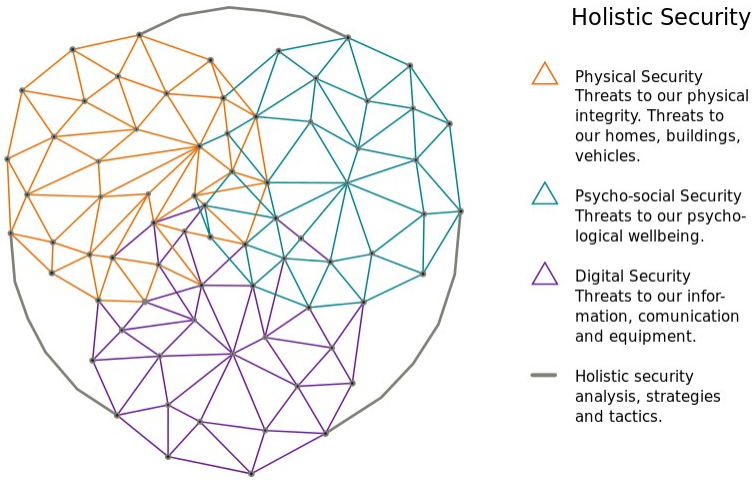
Input (15 minutes)

To summarise the discussion, draw out the importance of the need for human rights defenders to be aware of the security dimensions of their day-to-day activities in order to be able to identify threats relating to all domains of security.

Using concrete contributions from the discussion, draw out the interconnectedness of different aspects, such as:

- Better digital awareness enables better information security planning, which can reinforce one's perception of risk and security.
- Greater psychological awareness (e.g. around one's need for security, work-related risks and reactions in situations of stress) provides opportunities for more in-depth risk analysis and informed decision-making on risk mitigation measures.
- Regular analysis of your situation and context encourages individual and joint decisions on tactics and practices including digital security and well-being.

Where useful, visualise the interrelation of all dimensions of security (e.g. by reinforcing circles, spiral etc.).



If you have a good knowledge of the participants' context and consider there to be a strong feeling of trust in the group, as well as between the group and you as the facilitator, this may be a good moment to relate the insights from the discussion to incidents that participants have experienced personally.

Deepening (20 minutes)

Step 1. Group work (10 minutes). Have pairs of participants advise Olga and her organisation in preparation for her next trip. You may want to give some prompts, such as;

- What does she need to think of regarding her devices?
- What does she need to consider in order to feel more secure?
- What does she need to consider regarding the information she is carrying?

Step 2. Capture the outcomes of the group work on a flipchart or screen and highlight once more how different security aspects interlink.

Step 3. Highlight existing coping strategies and resilience that you may have observed in the trainees. Be positive (not admonishing) in your approach.

Synthesis

Relate the outcomes of the discussion to the focus of your training (i.e. digital security, psycho-social, organisational security management or well-being). Re-emphasise the interrelation of the three dimensions by referring to examples from the Olga story and the diagram you drew as useful.

Optional: Weaving the exercise throughout the training

The above scenario could be re-introduced throughout the course of the training to direct analysis

and reflection to particular aspects of risk assessment, for example:

Actor mapping: Who is affected by the work of Olga and her organisation? What position do they take towards her work? What strategies may they employ to support or harm Olga? Explore the scenario in a role play with participants taking the role of the security officials to investigate their intentions and strategies as adversaries to Olga.

Possible prompts:

- Why would they want to take the USB?. Just scare her? To access, copy, manipulate, or destroy the information on it? Or to plant malware on the device?
- What could they be looking for?
- What could they do with this information? Share it with other agencies? Use it against Olga and her organisation? Use it against other HRDs, victims and witnesses?.

Information mapping: Use the example of Olga as an entry point to support participants' information mapping in their own contexts. What information do participants currently carry with them or have access to? Who else has access to it? How is it shared with others? What information is considered sensitive for them? Where is that sensitive information stored? Is it backed up?

Incident response: Using the example of Olga, ask participants to consider how the organisers of the event, as well as Olga and her organisation, could react to the incident. Explore elements of response, reflection and organisational learning for Olga and others affected while thinking about restoring and maintaining well-being, information security and physical integrity.

Protecting Memory, Protecting Ourselves: Collective Memory as a Gateway to Understanding Holistic Security

Context

The concept of collective memory is familiar within many activist circles and may in some contexts provide the foundation of our activism. This can be especially important when the state and state-driven media are propagating an alternative 'truth' that undermines or directly contradicts lived truth as we have experienced it.

This session is an example of how to use a broader topic to introduce key themes into the training from a holistic perspective. (The same approach could also engage a different opening topic than the one used here, depending on the specific context of the participants.)

The session below is not designed as a self-contained workshop, but rather a first session to open a longer training (e.g. the first morning of a three day training). It provides context and entry points for a series of related security elements that could be covered in-depth during later sessions.

Objectives & Requirements

Attitude: Collective memory is a valuable platform for understanding security.

Knowledge: Understand the significance of collective memory and the steps that can be taken to secure it. This session provides a means to think about security from a holistic perspective, both personally and within a movement.

Skills: Identify sources which can be used in building and maintaining the collective memory of a movement. Critically assess "truths" which may be perpetuated by powerful actors but not correspond to our lived truths.

Duration: Variable—minimum 90 minutes

Prerequisites: See below

Technical Requirements: Be as creative as possible, using a large space (indoors or outdoors), something to mark a pathway either in a spiral or maze shape, Supplies could include masking tape, seeds, flour, sand, nuts or stones to mark the pathway; pens and paper, coloured markers, photographs, news clippings, etc.

Theoretical and Online Resources: N/A

Contributors: Hadi Al-Khatib, Ricardo Gonzalez, Erick Monterrosas, Daniel Ó Cluanaigh, Hannah Smith, Moritz Tenthoff

Activity

Option I – Walking through your personal journey

In this activity, participants individually create their own 'path' as a narrative of both their journey in activism and their personal lives up to the present and perhaps their desired future. (This path is represented on the floor with materials such as seeds, flour, sand, masking tape, etc.)

This activity is a very individual one. Participants are given at least 15 minutes to design their path and then take turns walking along it and presenting it to the rest of the group. The key to this session is self-reflection, allowing people to review what influences and events have led them to where they are now (particularly with reference to their activism), as well as to reflect on where their path may lead them next.

The activity can be influenced by the choice of shape of one's 'path'. This can be pre-set by you as the facilitator, or be left open for participants to create their own. For example,

- A **spiral** can be walked ideally first from the outside to the central point, beginning with where I am now and going backwards to the furthest desired point (maybe to the first key event that led to our activism, or even all the way through childhood to birth) before moving chronologically back out from the centre to where I am now and further, where do I want to go?
- A **maze** shape can also be used. In this case we have more autonomy over the path which we walk, we must perhaps also face pathways that lead to dead ends where we are forced to turn around.

Option II – Drawing our collective memory

This is a group activity where all participants collectively create a mural to represent their own shared history. The activity is similar conceptually to the 'Draw your Day' activity included in Session 1: Defining and Contextualising Security, but could encompass a much broader time frame and focusses on the experiences common to the group as a whole. The activity is easiest within a relatively homogeneous group, but could also be useful in defining common ground in a heterogeneous group too.

Step 1. On a large area of wall or floor space, spread out a number of sheets of flipchart paper. Instruct participants that they will collectively create a mural to represent their shared journey together. It can be a linear or narrative (with a clear timeline) or structured differently as the group prefers. In the centre, the participants could put a representation of what they are fighting for, what they stand for and/or who they are. This can be something that inspires them and reminds them of their principles throughout the training. On either side of this, they can map out their collective memory and the events, both positive and negative, which have led them to establish and fight for this vision.

Step 2. Give participants time, at least 10 minutes, to discuss what to put in the centre. In the other areas of the mural, they can work individually or in smaller constellations.

Step 3. Give participants 30-45 minutes to complete their mural and assemble the drawing on the wall.

Alternative variation: In groups where collaboration like this may be challenging, give each participant their own half-sheet of flipchart paper for them to draw their journey, and eventually

assemble the whole group's drawings together on one area of wall/floor. As an optional next step, participants can use string and pins to make connections between the moments they have experienced together to represent the interconnected nature of their individual journeys.

Option III – Reclaiming our history

When working with a group which struggles against a state that attempts to 're-write' their history through control of the media and other outlets, an interesting variation on this activity could be asking participants to bring news articles, photos and other media with them to include in the mural, in order to contrast the 'official truth' with their own lived experiences.

Discussion

The discussion should take place among the entire group to reflect on the experience of doing the activity, and eliciting any themes and feelings that emerged during the activity. The discussion should also touch upon what collective memory means to the group.

Here are some themes that may be useful for guiding the discussion:

- How HRDs establish an official narrative or historical truth.
- Lived experiences vs. official "truths", and who creates them.
- Structural influence on the way official "truths" are retold (e.g. victim blaming/shaming, gendered violence).
- The power of our narratives to influence who we are, how we got here and where we want to go.
- What the political, economic, social and technological trends have been, and how they have affected the group's work (see also Session 5: Situational Analysis, and the corresponding chapter in Holistic Security: a Strategy Manual for Human Rights Defenders[15]).
- Identifying trends, threats, vulnerable groups, methods of repression, and the group's capacities in view of these.
- Considering the role of justice within our movement, especially when this is not delivered through the judicial system.
- Making space for difficult memories and experiences (for both the group and individuals).
- The role of physical space within our collective memory and our activism. (This may also include a discussion of who controls physical space and how this control is often taken away.)
- The importance of naming perpetrators.
- How we preserve and protect our collective memory.

It is worth noting that for some groups the link between their current activism and collective memory is obvious, but for others, this link may not be immediately apparent. It is important for HRDs to see their work as the living form of their collective memory; recording, asserting and

15 https://holistic-security.tacticaltech.org/chapters/explore/2-2-situation-monitoring-and-analysis

protecting this memory, this subjective reality, should be seen as an empowering political act.

Input

Like the discussion above, the inputs in this exercise will depend greatly on what you are using the exercise as a vehicle for (i.e. the overall purpose of the training). Some themes and topics to highlight in almost any case would include:

- Security is personal. Just as we define our own goals as human rights defenders and activists, we also define security for ourselves. We build security together just as we build our movement(s) together. And when we protect ourselves and each other, we also protect the movement and what we believe in.
- Speaking our truth from our lived experience is political and sometimes subversive. Our truth is to be protected—sharing and celebrating it strengthens it.
- Evidence of our experiences—documentation, videos, pictures, news articles, files and so on—are therefore vital and need to be protected. This evidence directly links to information security.

Deepening

The deepening, like the input, will depend largely on what your objective for the training is. The question of how we preserve and protect our collective memory is incredibly important. This realisation can be very useful for opening the door to conversations about physical and digital security which may otherwise seem abstract or low priority. Many HRDs may have large data sets, video and photographic evidence, and objects which are significant to their evolving collective memory.

Some ideas for deepening are included below – refer to sessions detailed later in this manual or refer to the Holistic Security website for more information and guidelines on how to facilitate these sessions.

Situational Analysis: Participants could use this visualisation as a platform for mapping the Political, Economic, Social, Technological, Legal and Environmental trends around them, and thinking about how they collect this data, and from which sources.[16]

Actor Mapping: Participants could use this visualisation as a means of identifying their allies, adversaries and neutral parties relative to their work and their ideals, and then analysing them in terms of their interests and resources.[17]

Information Mapping: Particularly in groups working with evidence of human rights abuses, conflicts, etc., ,this exercise could be used as a platform for mapping how they are managing their sensitive information (e.g., where it is stored and under what conditions).[18]

Documenting and Reporting Violations (gender perspective): This exercise could be used to highlight the contrasting narratives of a patriarchal state/society vs. women and LGBTI human rights defenders, and the ways in which injustice is hidden behind patriarchal discourses.

16 https://holistic-security.tacticaltech.org/chapters/explore/2-2-situation-monitoring-and-analysis
17 https://holistic-security.tacticaltech.org/chapters/explore/2-3-vision-strategy-and-actors
18 https://holistic-security.tacticaltech.org/chapters/explore/2-4-understanding-and-cataloguing-our-information

Participants could use this exercise in order to come up with strategies on how to document, preserve and articulate their truth.

Below are some topics that you could link to in the discussion and follow up on in direct sessions later:

- secure data storage
- secure cloud storage
- physical storage, archiving, preservation of objects
- techniques and strategies for long term digital preservation.

Synthesis

The synthesis will depend on the deepening you choose.

Further considerations for this exercise:

- Confidentiality.
- Psychologically sensitive space.
- Awareness of emotions (our own and others).
- Have good resources prepared in case you need to offer referrals for participants acutely suffering from trauma.
- Gender-aware approach to personal and collective histories.
- Small groups can be better for trust and sharing than larger groups.
- Respect for the plurality of perceptions.
- Be aware of backgrounds in the group – homogeneous, heterogeneous/multiple backgrounds or conflicting identities.
- Awareness of conflict resolution skills and approaches.
- Guide conversations to identify trends and methods of repression, especially with vulnerable groups.

Security Considerations when Travelling

Note: This session is not exhaustive but provides an introduction to security considerations while travelling. The session focusses on teasing out best practices is not necessarily based in a risk analysis and/or current security policies that the participants may adhere to – it is best covered later in a training, once elements of context and threat analysis and security planning have already been taught and the training can focus on application in concrete scenarios.

Objectives & Requirements

Attitudes: Being alert and attentive to security when travelling. Critical awareness of security during the training itself.

Knowledge: Provide general awareness on security considerations while travelling. Identify areas of improvement that may require behaviour change, additional technical and non-technical skills and organisational policies.

Skills: Security analysis while travelling and when preparing for travel.

Prerequisites: N/A

Technical Requirements: N/A

Theoretical and Online Resources: Personal Security: A Guide for International Travellers[19]

Time: 120 minutes

Contributors: Bobby Soriano, with Rory Byrne, Sandra Ljubinkovic, Daniel Ó Cluanaigh, Ali Ravi, Nora Rehmer

Key to this session is making sure that you or the organiser send a **Travel Security Checklist** to the participants in advance as part of the training preparation. This is also in line with **walking the talk** which is a basic principle of holistic security. You will review this checklist with the participants in the synthesis part of the session.

Activity (30 minutes)

Draw your travel

Step 1. Give participants half-sheets of flipchart paper. Instruct the participants to draw how they travelled to the training, recalling as many details as possible such as:

- Getting the invite to the training (How did they receive it? By email, phone, etc.?)
- Preparing for the trip: What did they take with them? What and who did they leave behind?
- Finally leaving the house or office (whatever the case may be)

19 Tanya Spencer (2013) "Personal Security: A Guide for International Travellers", CRC Press https://www.crcpress.com/product/isbn/9781466559448

- Travelling (How? By foot, in a car, in a plane?)
- Who were they with? Who did they meet along the way?
- What did they eat? When did they sleep?
- Getting to the training venue (How did they feel?)

Step 2. Participants then pair together and describe their drawings to one another. Working together, they identify possible security incidents and indicators during the course of their trip to the training venue. Where is/was there a potential threat? How do they know? Ask them to consider things like:

- Your bags and what you brought with you: Who could have accessed them? How do you know they didn't?
- Your devices and information.
- Your well-being: did you rest and eat enough?

Discussion (15 minutes)

To start the discussion, participants report in pairs, present their insights and highlight the security items that they missed in their initial drawings. Then open up to the group for comments, questions and reflections.

Input

Travel tips and elements of a travel plan/checklist (30 minutes)

The next part of the session attempts to elicit what participants have learned during the activity. Options for structuring this content include organizing it by:

- Timeline – before travelling, while travelling, during the training and when travelling back home.
- Items to bring or not bring while travelling.
- How sensitive is the activity that you are travelling for? (E.g. highly sensitive, not very sensitive, etc.)

General tips for international travel

The following is a **non-exhaustive** list of tips that may be useful when travelling across international borders:

Starting out on a trip

- If the trip is potentially stressful, have a **transition ritual** where you take the time and space necessary to 'transition' into the next phase of your work. This is a personal practice and its nature will vary from person to person.
- Consider what resources you need to take with you for your emotional well-being:

sentimental items, pictures, jewellery, etc.

- Have enough cash for emergencies.
- Avoid connecting to free, open wireless networks in airports and other transport hubs, unless you have a VPN or use TOR.
- Consider using tamper tape on your bags and devices (USB ports, hard drive covers) so that you know if they have been tampered with.
- Avoid sending sensitive messages via SMS from areas in or near airports, as they are likely to be monitored.
- Remember to bring chargers for your devices.
- Consider buying a World SIM that you can use in a large number of countries.
- If it's a long trip, consider bringing some of your own food and a cushion (or similar items) to avoid discomfort.
- If travelling in a group, consider travelling by different routes to not attract attention.
- Consider what resources you need to take with you for health, recreation or relaxation (e.g. medication, running shoes, sports equipment).

At border crossings

- If necessary, agree (in some detail) about a 'back story' with colleagues. Be careful! Being caught lying may be worse than a 'true story' about attending a training or conference. If you have 'back story', be sure to have some supporting evidence when you leave the country, as you may be asked questions again.
- Agree on a meeting point and time with your colleagues.
- Provide only minimal information when asked for it.
- Be polite but firm.
- Stay with your belongings.

At your destination

- Relaxation and energy management: Make clear, dedicated spaces for relaxation and stress relief (according to your own needs) that are non-negotiable except in emergencies.
- Avoid walking alone at night.
- Consider advising hotel staff not to provide information about you.
- Avoid meeting unknown people at locations you don't know well.
- Memorise phone numbers of sensitive contacts rather than save them in your phone.
- Agree on a simple 'discreet signal' to alert your colleagues of an incident.
- Separate sensitive information on devices.
- Type up any handwritten notes you take before travelling again.

- Send notes digitally to yourself or to colleagues, and consider encrypting them.
- Consider using shorthand or code names when writing by hand.
- Consider securely deleting unnecessary sensitive information from devices.

When leaving a country

- Ensure all paper with sensitive data is disposed of safely.
- Assume you will be searched.
- Have files backed up remotely if possible.
- Agree on your story. It should be consistent with whatever you said when you entered the country.
- Stay with your belongings.
- Consider transporting sensitive data on a MicroSD card which is easier to conceal if it can't be stored safely online.

Creating a plan/checklist

This session can also be used as an example of applied security planning. It may also be useful to include the basic elements of a security plan:

- The objective of the activity.
- The threats identified.
- Preventative actions and resources (before, during and after).
- Response and emergency actions and resources (before, during and after).
    - Including: WHEN is it an emergency? WHAT defines an emergency?
- Communication and devices.
    - What kind of sensitive information will you have during the activity? Which devices is that information on?
    - Who can access it? How?
    - How can you protect it?
- Well-being and self-care.
    - Adequate food, rest and relaxation.

Deepening (40 minutes)

Create a plan/checklist

Either individually or in groups, participants create a basic travel security checklist and/or plan for themselves. They should consider the input shared during the session (and may mirror whatever

structure you've used during your session). They should aim to create something that they can refer to the next time they travel.

Step 1. Give participants 20 minutes to create an initial plan and checklist (at minimum).

Step 2. Allot 10+ minutes for questions and answers ('Q&A'). Participants don't have to share their plans, but may have questions or want to compare their plans with others.

Step 3. Allow participants to complete their plans for a further 10 minutes based on what was shared during the Q&A.

Optional: Participants can go beyond the personal to identify organisational security aspects. They can later bring possible organisational policies back to their organisations as an entry points for discussion.

Synthesis

The function of a synthesis is to summarise and recap the key learnings of the session and answer any outstanding questions the participants may still have. Take this opportunity to remind the participants about the security travel checklist that was sent to them before the training, and as an optional further deepening, have a brief discussion about it and see if it captures some of the items discussed in this session. This can also be useful feedback for the organisers of the training.

Communication Security: An Introduction

This session can be an introduction to several topics with some minor modifications on the content and focus. Some related sessions that this can be of use as an introduction could include

- Mobile security
- How the internet and mobiles work.

Objectives & Requirements

Attitudes: Emphasize the importance and primacy of awareness over tools or technology.

Knowledge: Understanding of how digital communications work and their inherent insecurities in a non technical way.

Skills:: Basic assessment of digital communications security.

Prerequisites: N/A

Technical Requirements: Flipchart, whiteboard, postcards/paper, coloured paper, stickers, pens, markers.

Theoretical and Online Resources: Security-in-a-Box (https://securityinabox.org), Trackography (https://trackography.org)

Time: 60-80 Minutes

Contributors: Sandra Ljubinkovic, Daniel Ó Cluanaigh, Ali Ravi, Nora Rehmer, Bobby Soriano

Activity & Discussion

Option I – What is the internet? (20 minutes)

This is an 'keyword identification' activity. It starts off with a word-association game, similar to 'What is Security?' (Session 1: Defining and Contextualising Security).

Step 1. Ask the participants to share words that come to their mind when they hear the word 'internet'. Encourage participants not to 'hold back' but to respond as spontaneously as possible, without thinking.

Step 2. The facilitator notes the words down on flipchart paper or a whiteboard.

Step 3. Highlight the words related to communications that emerge from the group. Emphasize that most of the activities that we do on the internet are largely about communications. (There has to be some agreement with the participants that this is the case. If there are other ideas that have emerged, you can have a discussion to further clarify those ideas and arrive at some agreement(s) and consensus.

Option II – The postal service (30 minutes)

Step 1. Divide participants into three groups. Two groups will be communicating with one

another, and one group will be the 'postal service'.

Step 2. Tell participants that we are going back in time to before the internet. How did we communicate back then? With the postal service!

Step 3. Hand out the following materials to the two groups communicating with each other: postcards, sheets of white and coloured paper, pens, tape, stickers, etc. Instruct each group that they have to send a message to the other group using the postal service. The message that they send needs to include routing information, including the senders' information and the recipients' information. When their message is written, they can call the postal service to come and collect the letter and they will deliver it.

Step 4. While these two groups are writing, instruct the postal service group to gather as much data as possible about the messages.

Step 5. After the first round of communications is complete (the first message sent, and one response received), , allow one more exchange of messages between the two groups. Remind the participants to find ways of protecting their communication if they feel it might be monitored. (This can include using other materials, the content of what they send, etc.).

Discussion: After a couple of rounds of communication back and forth, ask the postal service to report back on what information they have gathered. How did they get this information? How did the two groups attempt to protect it, and what were the advantages and disadvantages of each method?

Input (20 minutes)

Elements of a communication process

The discussion that follows after the activity will focus on the elements of a communication exchange.

The main idea is to emphasize that digital security is not simply about technology and tools, but largely about awareness. Security awareness should precede tool usage. An informed appreciation of security awareness should guide tool usage.

Sender and receiver: The participation of all communicating parties is essential in every communication. This can be one-to-one, one-to-many and many-to-many. Remember that security is more difficult to maintain when more parties are involved. When talking about security in respect of the sender and the receiver, this is almost always a trust issue and no technology can provide a solution to this aspect of communication. This involves the individuals that send and or receive the information. In some cases simply communicating with a specific individual or organisation might put your security at risk and vice versa.

Message: At first glance, the message is simply the information that you communicate. The focus is usually the **content** of the message, and rightly so since this is one of the main concerns when talking about security. However, it is important to note that lots of information about each message is generated when communicating and this is equally as important. Information about the message (or information about information), called **metadata**, is information that surrounds the actual message. Metadata includes information such as the sender and receiver, or the date an email was sent – without which it wouldn't be possible to send the message in the first place.

But metadata can reveal information that might compromise your security – such as your location

or contacts. Securing your communications is therefore both an awareness and tool concern. Using encryption is good for hiding the content of your message but at the same time you might be compromising your security through your metadata, which can't be encrypted, or raising red flags by using encryption in the first place. End-to-end encryption hides the content of your messages from everyone except your intended recipient, but this does not hide the fact that you are using encryption. Remember that hiding information is very different from hiding the fact that you are hiding information

Channel: A 'channel' is the medium through which a message is conveyed from the sender to the receiver. Spoken words travel as sound waves through the air, while letters can be sent and received via the postal service. In these examples the air and the postal service each act as the channel. There are numerous channels for digital communications, but for our purposes we will focus on internet channels and services.

- Internet channels are often owned and provided by corporations such as internet service providers and telecommunications companies. We and our information are subject to how these channels are set up and secured by the service providers. Although we do not have control over how these channels are secured, we can improve our awareness of how the system works and make decisions about which providers we deem most trustworthy.
- Services include things like email and social network subscriptions. Most if not all internet services are subject to laws of the country where their systems are physically based and the country in which the company is legally registered – not the country in which the user is based.

Location: Location is a very important piece of metadata that accompanies internet communications. For any communication to take place the sender should be able to know the receiver's location and vice versa. It would be very difficult if not impossible to communicate if you do not know the location of the individual you are communicating with - much the same as if you wanted to post a letter but did not know the address of the intended recipient. Prior to the internet this element was largely about your physical location, i.e. you physical postal address. This is no longer true; it has extended to mean our virtual locations based on the services that we use and subscribe to on the internet. Email addresses, your social media accounts are locations on the internet, which are identified by IP addresses (Internet Protocol addresses). These often correspond to concrete physical locations. Like houses and offices, virtual locations such as email and social media accounts can be subject to theft and attack. This element is both an awareness and technology concern. There are tools that can help you hide your location and provide you some level of anonymity to hide your identity.

It may be useful to accompany this with a short demonstration of **Trackography**[20] so that participants can visualise how data travels across the world when we browse the internet.

Protocol: This is how and what you use to assemble and transmit your message through a specific channel. There are different protocols used depending on how you are connecting to the internet. For example, accessing messages via a browser (e.g. Firefox or Chrome), an email client (e.g. Thunderbird, Outlook) or another type of application. Most protocols don't hide your identity but some protocols do hide (encrypt) the content of your message. Examples of internet protocols using a browser include **HTTP** and **HTTPS**. HTTP is the default language that allows your browser to communicate with a webserver, i.e. the way that the data from most websites is assembled and travels across the internet to your browser. HTTP does not hide your communication and any information transmitted can be seen by your channel provider or whoever has access to that

20 https://trackography.org/

channel. HTTPS on the other hand allows you to hide (encrypt) your communication, so only the browser and the web server can see the message.

Of course the process is more complicated than this, but what is important to note is that most protocols are concerned with the security of the message *content,* but not the security of the metadata that accompanies the message as it is sent and received. The **content** of a message can be unavailable to a third party surveilling your communications, but the **metadata** of your message includes information about your physical location when you sent a message, the time you sent a message, and other details.

Another thing to remember is that protocols should be known and used by the systems and channels sending, receiving, and rendering your messages. For example, your browser is 'HTTPS aware', meaning it can understand and use HTTPS, but the server of a website must provide HTTPS in the first place in order for you to benefit from it. If the web server does not provide HTTPS, then HTTPS communication will not be possible. On the channel side, the channel must also be able to facilitate HTTPS communication. Most internet channels allow HTTPS but in some cases this protocol is not allowed and is filtered or blocked.

Context: The context is the environment or situation in which your message was sent and delivered. This is largely a political and social question rather than a technical one. However, understanding your context is always helpful to determine the security of your communication. Doing a risk assessment is a first step in understanding your context and effectively securing your communications.

Deepening (20 minutes)

Prioritising sensitive elements

This can be an activity/exercise where in the participants provide examples for each of the elements based on the **Input** section above. The aim is to have the participants deepen their understanding of the different elements by relating these to their personal experiences and organisations that they work with.

Participants can, either individually or as a group, fill in a sheet of paper or flipchart wherein each category (above) is marked clearly. The questions to pose for each are:

- **Sender/receiver:** Which contacts are sensitive? Which connections would we rather not disclose or make public?
- **Message:** What content is most important for us to protect (even if it draws attention to us)?
- **Channel:** What channels and services do we use to communicate? Do we trust them? Can we change any of them?
- **Location:** Is our location sensitive when we communicate? (when/where?)

Outline again the options which are available to increase communication security:

- **Sender/receiver, location:** VPNs and TOR
- **Message content:** HTTPS, GPG and secure chat (Jitsi, Pidgin)
- **Channel:** Alternative providers to Google, Facebook, etc. (Riseup, Autistici, Diaspora)

This information can be used as the starting point for deciding which technical and tool-based needs exist in the group, and later, developing a communication policy.

Alternative: This section can run as an activity, mapping out the different elements of communication. Each individual or a group of participant/s can act out a specific element and identify ways to make communication insecure and also make information secure. The end of the exercise can be can be a short list of both insecurities and ways to be more secure.

Synthesis:

- The internet is primarily a communicative tool. Even browsing a website is a form of communication.
- Protecting communications is not just about protecting the content; metadata may also be sensitive.
- Protecting content and metadata can also draw attention to us.

Part III

Holistic Security Context & Threat Analysis Exercises

Contents

Introduction

The Holistic Security Context & Threat Analysis exercises which are set out in this section are designed to form a sequential 'flow' based on the material from **Holistic Security: a Strategy Manual for Human Rights Defenders**. It is therefore suggested that they be carried out in order over a training of four or more days.

The sessions were developed for and tested at two four-day 'Introduction to Security' trainings held at the Centre for Training and Networking in Nonviolent Action "Kurve Wustrow" in 2015. They do not, however, represent the totality of potential sessions that could be created based on the manual. As such, we would encourage facilitators to take inspiration from the themes, approaches and ideas put forward here to develop and share further sessions designed to suit the needs of the groups they work with.

All the structured learning sessions in this manual are organised according to the **ADIDS (Activity-Discussion-Input-Deepening-Synthesis) approach**,[21] an adult learning methodology. The ADIDS approach plays on the many different ways in which adults learn, allows participants to take an active role in their learning, to contextualise for themselves what is being learnt and why, and to better internalise new content. Each session guide also details the **knowledge**, **attitudes** and **skills** which comprise the major learning outcomes for the session. Refer back to the Introduction in Part 2 for a description of the individual components which make up the ADIDS approach.

21 For more about ADIDS, see https://www.level-up.cc/before-an-event/levelups-approach-to-adult-learning/#the-adids-approach

Session 1: Defining and Contextualising Security

Objectives & Requirements

Attitudes: Security is personal and subjective.

Knowledge: Basic security awareness in daily life; basic understanding of threats and existing security practices.

Skills: Basic security analysis methods.

Prerequisites: N/A - this is a good introductory exercise.

No. of Facilitators: 1

Technical Requirements: Flipchart, coloured markers, other art materials.

Theoretical and Online Resources: Integrated Security Manual (http://www.integratedsecuritymanual.org/)

Time: 80 minutes

Contributors: Sandra Ljubinkovic, Daniel Ó Cluanaigh, Ali Ravi, Nora Rehmer, Bobby Soriano, Peter Steudtner.

Thanks to: Cheekay Cinco. Partially based on content from the Integrated Security Manual by Jane Barry / Kvinna till Kvinna.

Activity (20 minutes)

Draw your day

Step 1. Participants are given a half sheet of flipchart paper each.

Instructions: Draw a typical, active working day for you in your activism, from when you get up in the morning until you go to sleep at night. Consider:

- When you wake up, and the rituals you have to start the day (e.g. where are you, who are you with, etc.)?
- When do you leave your home? Where is the first place you go? What do you take with you (e.g. mobile phones, handbag, etc.)?
- Where do you go, what does the journey look like? Who else is there?
- Think about where you are when you're working. Who are you working with? What devices are you using, if any?
- Do you eat or relax during the day?
- How do you get home? Or what do you do before you go home?
- What do you do in the evenings? When do you sleep?

Give participants approximately 15 minutes to make an initial drawing. Remind them that there is **no obligation to share the drawing itself** and they do not have to impress anyone. The exercise is simply a way of reflecting on existing habits and relating them to our security.

Step 2: Allow 5-10 minutes for participants to reflect on anything that occurred to them during the process.

Discussion (15 minutes)

What is security?

Step 1. Get participants to take a break from drawing for a moment, to perform a quick word-association exercise. Word association can be useful, because there is often great honesty in our initial reactions to concepts.

As the facilitator, you will give a word for participants to respond to. Ask them to respond quickly with whatever they associate with that word.

Step 2. Give an example to get participants to shout the words that spring first to their mind. You can repeat this a couple of times with different words if it's helpful to get everyone warmed up. (For example, ‘elephant’.)

Step 3. Give the real word: 'Security'

Step 4. Participants will respond with many different words. Write them on a flipchart to the extent possible. Give up to 10 minutes for this.

Optional step: Some minutes into the exercise, emphasise that participants should respond to what security means to them personally. You may note a major shift in the kinds of words which come up.

Notes to share with participants:

- This exercise tends to be unique with every group: this is because security is fundamentally a personal concept that we must define for ourselves in the context of activism which puts us at risk.
- Many of the words we associate with security will have positive connotations, while others may be associated with militarism and conflict. It is important that we reclaim the meaning of 'security' for ourselves and for our human rights work.

Input (10 minutes)

Security as personal and holistic

Many of the words which came up in the association exercise may have been connected to family, friends, finances, freedom, and other concepts. These relate to our most fundamental desire for well-being, which is entirely subjective and defined by ourselves. We give our own meaning to security when our work involves making decisions and taking actions that can result in threats to us from others. Ultimately, our aim in this or any other security-related training is to strengthen our ability to protect our well-being. Any security measures which don't fortify our well-being are counter-productive as when our well-being is neglected, our overall security is weakened.

Many of the words may relate to the security of physical spaces, structures and vehicles. This is somewhat less subjective and more concrete. The security of particular physical objects can be very useful. For example, how to keep our offices more secure from theft or break-ins. However, we should only build these skills to the extent they are useful to us.

Many other words will relate to digital and information security. Digital security can be more objectively or 'scientifically' determined. For example, you can rigorously test information systems and devices. But once again, we should only engage with digital security tactics and tools to the extent that they are useful in our work and supportive of our well-being, because knowing our information is protected can be a great source of comfort for us.

Deepening (30 minutes)

Identifying threats and strategies

Step 1. Participants return to their drawings.

Look at your typical day and identify where you see danger or the potential for danger in your day. Consider your well-being and health, as well as the physical spaces you're in and the devices you're using.

Step 2. Allow 5-10 minutes for this and another 5-10 minutes for further reflection. This may be a conversation in which participants share their vulnerabilities, so be sure not to cut them short.

Remember: You are not there to have the answers to all problems. But it is positive to openly recognise that participants are now taking an empowering step to organise and improve their security situation.

Step 3. Participants return to their drawings.

Look at your typical day and identify where you see strategies, plans, tools, tactics that you already use in order to stay safe and protect yourself. Give 10 minutes for this and allow an additional 10 minutes for reflection.

Synthesis

Points to highlight from this exercise as you close:

- Security is personal and subjective – we define it for ourselves.
- Our well-being should be the fundamental reference for security.
- We already have many existing tactics and considerable resilience in order to continue our work despite the challenges we face.
- With that as our starting point, we can go forward into analysing our work from the perspective of digital, physical and psycho-social security in order to improve our security situation.

Session 2: Individual Instinctive Responses to Threat

Objectives & Requirements

Attitudes: Understanding stress management as something which helps us manage our security better.

Knowledge: How threats and stress affects us, physiological responses to threats and ways in which they may help or hinder us.

Skills: Organised approach to stress management, including increased ability to identify symptoms of stress in ourselves and tactics for reducing stress.

Prerequisites: N/A

No. of Facilitators: 1

Technical Requirements: Flipchart, whiteboard, Activity images on paper (lion, horse, turtle), hand-out on Physiological Responses to Threat and the Stress Table

Theoretical and Online Resources: Holistic Security: a Manual for Human Rights Defenders

Time: 90 minutes

Contributors: Craig Higson-Smith, Sandra Ljubinkovic, Daniel Ó Cluanaigh, Ali Ravi, Nora Rehmer, Bobby Soriano, Peter Steudtner.

Activity (20 minutes)

Lion, Horse, Turtle

Step 1. Divide the space into three areas by placing pieces of paper on the floor that read lion, horse, and turtle.

Step 2. Ask participants:

- What are the characteristics of lions? How do they respond to danger? (Typically by attacking.)
- What are the characteristics of turtles? How do they protect themselves? How are they different to lions?
- What are the characteristics of horses? How do they protect themselves? How are they different from the others?

Step 3. Gather participants in the centre of the space and ask them to think of a particular event when they felt in danger. Leave a moment for them to think, and give hints if necessary (e.g. during a protest, or a security incident that they have already discussed with the group).

Step 4. Now, ask participants to move towards the animal with which they associate their behaviour in that moment.

Discussion (10 minutes)

Step 1. Lead a 'popcorn' style discussion on the exercise you just completed. If needed, use prompt questions such as:

- Why did you associate yourself with that animal in that situation? How did you act?
- Was it a conscious or unconscious decision to act the way that you did?
- Did you always react in the same way, or has it been different in other situations?

Note: Although the energy can be light and fun in this conversation, people may recall particularly difficult moments when they experienced violence. They may also have some feelings of sadness, guilt or shame for their actions. Try to avoid value judgements between the different archetypes and avoid critiquing how someone behaved in a particular situation, but rather listen respectfully to their rationale for doing so. If people are hesitant to talk about their own experiences in detail, do not push them to share more than they feel comfortable with.

Input (20 minutes)

Physiological responses to threat

Humans, like all animals, have built-in responses to threats that have helped us survive as we've evolved as a species. When we perceive acute danger, many of these responses kick in without our being able to control them: they are hard-wired to our bodies and minds.

Introduce the following reactions on paper or a flipchart one by one. Then ask participants if any of the reactions particularly resonate for them, or if they have any reflections to share.

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.

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.

The 'comply response' involves doing what an aggressor instructs in the hope that our cooperation will result in the attack ending quickly and without injury. We might agree to suspend or abandon certain objectives or activities, or give up passwords to secure information.

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

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. For example, by telling aggressors about our families we might try to humanize ourselves in their eyes, a strategy that is sometimes useful in reducing violence.

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 threats of violence in order to publicly embarrass our adversaries.

The 'fight response' is when a person attacks with the intent of driving off or destroying an aggressor. (There are many ways to fight, and we all make our own ethical choices about this.)

If we have been through dangerous, stressful or traumatic experiences, sometimes these reactions can kick in when we are stressed or frightened, even if there is no 'real' danger present. Therefore, it is a good idea to look for indicators in our behaviour when we are under stress, and to work with them in order to reduce our stress.

Deepening (30 minutes)

Stress table[22]

This is a useful tool that can help us identify the effect(s) that stress has on our bodies and minds and apply our own tactics and resources for managing it.

Step 1: Ask participants to take a sheet of A4 paper and divide it into 16 sections. On a flipchart, draw a matrix (overleaf), with headers titled Indicators, Tactics, and Resources for participants to copy.

For the purposes of this exercise, we've identified three 'levels' of stress:

- **Green:** Bearable, motivating stress. This kind of stress might keep us creative, but we may tire easily, require more breaks and take measures to avoid sustaining this stress for a long period of time.
- **Yellow:** Unpleasant stress. With this level of stress we may feel both tired and 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 that 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 friends and family, and our intimate relationships. This level of stress also reduces the pleasure and relaxation that we enjoy 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.

22 https://holistic-security.tacticaltech.org/chapters/explore/2-7-security-indicators

	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			

Step 2. Ask participants to consider what **symptoms** each level elicits for them, however they define this for themselves. If you feel comfortable doing so, share an example from your own life.

Step 3. Ask participants to describe the tactics they use for either easing these symptoms or addressing the source(s) of stress, including the resources they need for this.

Participants fill out the sheet individually (10-15 minutes). They can share reflections with others, but sharing should be optional.

This table can serve as a guide for participants, and they can take it with them. It can help during planning to ensure they have access to resources to help them remain calm.

Synthesis (10 minutes)

Points to highlight from this exercise as you close:

- Security is not just an abstract concept—our bodies have evolved ways of keeping us safe.
- However, our bodies' reactions are impacted by stress, tiredness and trauma. In order to improve our security, we need to take steps to manage and reduce these.

Session 3: Group Responses to Threat

Objectives & Requirements

Attitudes: Understanding stress management as something which helps us manage our security better.

Knowledge: How threats and stress affect groups. Understanding of physiological responses to threat, and how they may help or hinder group processes.

Skills: Recognising negative reactions to stress within a group. Developing strategies to mitigate threat and identifying resources needed to implement these strategies

Prerequisites: N/A

No. of Facilitators: 1

Technical Requirements: N/A

Theoretical and Online Resources: Holistic Security Manual[23], Front Line Defenders Workbook on Security[24], and Protection International's Protection Manual for Human Rights Defenders[25]

Time: 45-60 minutes

Contributors: Daniel Ó Cluanaigh, Peter Steudtner

Thanks to: Magdalena Freudenschuss, Craig Higson-Smith

Note: This exercise is most useful for introducing a series of steps for context and risk analysis, and may be followed by individual sessions on these steps.

Activity

Draw your decision-making structures

In this activity, participants draw the structure of their organisations or groups both 'in theory' as well as 'in practice' when they are under stress. You'll use this to highlight how threats and stress affect the group dynamic.

Note: This activity is probably best if the group is made up of participants from different organisations. If the group has participants from the **same** organisation, it is important to ensure that all participants feel that they have a safe space for sharing or have the option to do the exercise anonymously. There are a number of reasons for this, including the power dynamics that exist within all groups and organizations.) If the group is made up of participants from the same organisation, the reflection afterwards may require some strong facilitation.

Step 1. Explain to participants that you are going to ask them to draw the structure of their groups,

23 https://tacticaltech.org/holistic-security
24 https://www.frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk
25 http://protectioninternational.org/wp-content/uploads/2012/04/Protection-Manual-3rd-Edition.pdf

including decision-making structures, both in theory and practice.

Step 2. Draw an example of an organisational structure and processes (like a basic organisational chart) 'in theory'. Then illustrate how that structure changes when an organisation is under threat or high levels of stress. It can be useful to use an example from your own life, but don't go into too much detail about a specific organisation.

Step 3. Give participants sheets of paper and markers and ask them to do the same for their own organisation. Give them 15-20 minutes to draw and reflect.

Discussion

This should be an open popcorn-style reflection, as some participants may not wish to go into details. Prompt participants to share how they feel their organisational or group dynamic changes due to threats and danger, or high levels of stress.

Input

Threats and stress affect group dynamics in a number of ways, and this varies greatly due to organisational culture and many other factors. There are some common reactions, however. Consider these potential changes to group dynamics under stress and see if they resonate with participants.

Harder group boundaries

One predictable change experienced by groups under threat is the boundaries that define the group becoming less permeable. Those 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 such changes can be protective,, there are also some potential difficulties with this. The impermeable boundaries of the group may distance the group from existing and potential allies, leaving it more isolated than it might otherwise be. These boundaries also reduce the flow of information into and out of the group. This may result 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 with those 'outside' of their group.

Less permeable boundaries also make it difficult to leave groups. Members who wish to leave might be branded as traitors or sell-outs in a way that is harmful to the individual and those 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 security.

Fixed patterns

Secondly, patterns of behaviour become more fixed and harder to change. This makes it more difficult for members of the group to question (supposedly) shared beliefs, or challenge the behaviour of other members. When we lose the ability to question each others' 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 for groups to 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 reduced levels of information exchange within the group, and fewer opportunities for group members to check their perceptions 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 the group boundaries may prevent victims of such abuse from escaping. 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 into the links between decision-making processes and security, we should not underestimate the positive effects of having fair and transparent decision-making processes. If a group has shared knowledge and responsibilities, it reduces the impact when perpetrators target the leaders of a group.

It may be useful here to create a safe space for participants to talk about mistrust and potential infiltration in their groups or organisations. How does mistrust affect the group dynamic? Allow the group to share their responses to these particular reactions to stress.

Deepening

For the deepening exercise, ask participants to begin to imagine:

- a vision for changing their decision-making structure(s)
- strategies for dealing with threats.

They should also consider the key resources they would need in order to facilitate this. This time, allow them to share this in small groups of two to three participants.

Finally, allow a space for any particularly interesting points to be shared back with the entire group.

Synthesis

Points to draw out of this exercise during the synthesis include:

- Threats do not just affect individuals. It also has an effect on the dynamics in a group or organisation. These dynamics are not always healthy and could in fact lead to further risk.
- A space needs to be created where group members can express and explore how threats impact their work and communicate non-violently about it, without fear of reprisals from higher-ranking or privileged group members.
- It is only after recognising potentially negative patterns that they can then be addressed appropriately.
- Once a safer space within the organisation has been established, it will be much easier to weave security practices into the organisation's work.

Session 4: Introducing Context and Risk Analysis

Objectives & Requirements

Attitudes: Context analysis is key to making informed decisions.

Knowledge: Essential steps of context and risk analysis. Awareness of existing strategies and tactics for security, protection and well-being. Structure of subsequent exercises in the workshop.[26*]

Skills: Basic context and risk analysis

Prerequisites: N/A

No. of Facilitators: 1

Technical Requirements: Flipchart/whiteboard and markers. If desired, coloured paper rectangles for writing session steps on.

Theoretical and Online Resources: Holistic Security Manual[27], Front Line Defenders Workbook on Security[28], and Protection International's Protection Manual for Human Rights Defenders[29]

Time: 45-60 minutes

Contributors: Sandra Ljubinkovic, Daniel Ó Cluanaigh, Ali Ravi, Nora Rehmer, Bobby Soriano, Peter Steudtner

Thanks to: Magdalena Freudenschuss, Craig Higson-Smith

Discussion & Input (45-60 minutes)

For this exercise, you will take participants through context and risk analysis, eliciting from them the measures they already take, and working backwards through the threats they identify (which lead them to take these measures), the sources of information they use to ascertain the presence of threats, the actors which pose these threats, the sensitive information which could be of value to their opponents, the purpose they see in their work, and the original problem which drives them to act for change. By taking this 'reverse' approach, you can demonstrate how the group already have security strategies in place which they have developed based on context and risk analysis – no matter how informally it may take place, while introducing a concrete framework which can be used to formalise their context and risk analysis.

Over the course of the discussion, you will write up the answers supplied by the group on a flipchart or butcher block paper. Below is an example of how the content should be laid out by the end of the session. Detailed steps to facilitate this exercise follow.

26 This exercise can be useful in introducing a series of steps for context and risk analysis, and may be followed by individual sessions on these steps .

27 https://tacticaltech.org/holistic-security

28 https://www.frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk

29 http://protectioninternational.org/wp-content/uploads/2012/04/Protection-Manual-3rd-Edition.pdf

Establishing problem		SITUATIONAL ANALYSIS
Purpose (WHY?)		VISION & ACTIONS
Actors & methods		ACTOR MAPPING
Sensitive information		INFORMATION MAPPING
Sources of information		SECURITY INDICATORS
Corresponding threats identified 1: ..... 2: 3:		THREAT IDENTIFICATION/ ANALYSIS
Suggested security measures: 1: ..... 2: 3:		STRATEGIES, TOOLS & TACTICS

INTERCEPTION

Step 1. Ask the group to imagine that they are preparing to attend a public protest. What are **three** security measures they take? Allow this to be a 'popcorn-style' discussion. Prompt with a question about which devices they would choose to take with them or leave behind.

Write the three suggested measures from participants at the bottom-left of a sheet of flipchart or butcher block paper.

At the bottom-right, in a different colour, write Strategies, Tools and Tactics.

Explain to participants that we are starting at the end. Each of us already has strategies, tools and tactics that keep us safer at a protest. What we will now do is explore how and why we came to these conclusions.

Step 2. For each of the suggested security measures offered by participants, ask:

- Why would you do this?
- What are you protecting yourself against?

Participants will respond with a number of suggestions (e.g., taking a gas-mask in case of a tear-gas attack; not bringing a mobile telephone in case of device confiscation during arrest, etc.).

Write at least one of the threats related to each of the strategies on the left side of the flipchart.

On the right, write Threat Identification/Analysis.

Discuss how we have taken these decisions because we have identified threats. (For example, the threat of potentially harmful events during a protest.)

Step 3. Ask participants: Why do we feel like these are things that could happen to us during a protest?

Participants will respond with answers such as: “it's happened before,” “we've read about it,” “other people have told us,” or “you see the police approaching with tear gas projectiles.”

On the left of the flipchart, write the sources of this information that participants give.

On the right, write Security Indicators.

Note that they have observed their surroundings and examined a number of sources of information—friends, colleagues, the media, etc.—in order to establish that these are the most likely things to happen to us. So we have (already) shared and analysed security indicators.

Step 4. Ask participants who they think is behind these potential threats. Who would carry them out?

Write responses on the left of the sheet. Focus on any of the tactics they have that relate to devices: Why did you make this decision? What are you trying to protect, or what might be at risk here? Participants may respond with certain types of information stored on their devices. Write this on the left of the sheet as well.

On the right (above) write: Actor Mapping, and below that write Information Mapping.

Discuss how we are generally aware that in most dangerous situations (such as this), there are actors who are our **opponents** and others who are our **allies.** (You can pause to ask for examples of who these are.) This awareness of allies and opponents means we've done **actor mapping**.

There are always struggles for information involving our allies and adversaries, including surveillance or access to our digital devices. We have less instinct for digital threats and attacks, making it vital that we conduct some **information mapping** to increase our safety.

Step 5. Ask participants, why we would be at a protest in the first place. What's our objective (or what are common reasons for attending protests)?

Answers might include 'justice', 'demanding rights', etc. Write their answers on the left.

On the right, write Vision and Actions.

Describe how as human rights defenders, we have a vision of the positive change we want to see in our society, and we decide what actions to take in order to try to achieve that vision.

Step 6: Ask participants, how did we establish that there was a problem to address in the first place? How do we monitor our progress and changes?

Write participant answers on the left. On the right, write Situational Analysis.

Consider that we're constantly analysing our surroundings, beginning with our personal experiences but also through secondary and tertiary sources of information such as friends, colleagues, and the media. This is **situational analysis** and informs our strategies for action in defence of human rights.

Synthesis (5-10 minutes)

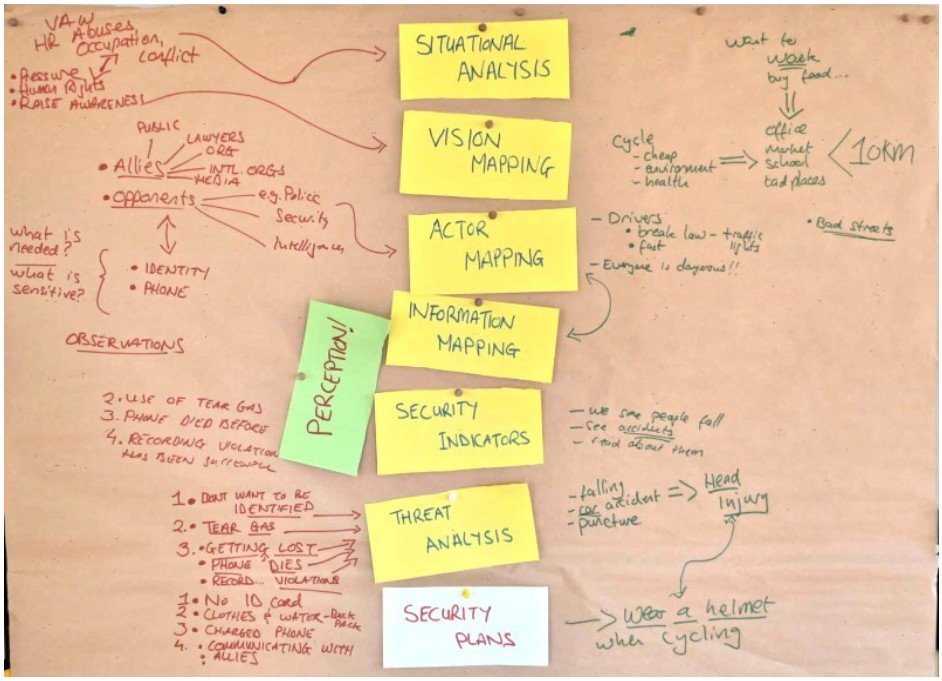
Refer to the complete list of steps and answers. These are the basic steps of context analysis – we carry them out all the time. As human rights defenders, it can be useful to simply be more organised and systematic about it given that we often face threats as a result of our work.

- Each of these steps can be an exercise that we should carry out regularly in order to **update our security strategies, plans and tactics according to the changing context in which we're operating**.
- This looks like a scientific, rational process, but,**it's not**. One of the biggest challenges we face is related to our **perception and well-being**. If we are stressed or very tired, we may find this process very difficult to do. We need strategies both for managing stress and exhaustion, as well as checking our perceptions with trusted colleagues or partners. We may discover that we have **unfounded fears** (which some call 'paranoia') or **unrecognised threats** (i.e., verifiable threats that we didn't perceive before).

Write Perception vertically alongside the steps of context & risk analysis.

Allow space for questions and discussion as needed.

Sample completed flip chart (with additional example on right)



Session 5: Situational Analysis

Objectives & Requirements

Attitudes: Seeing value in analysing the political, economic, social and technological context from a security perspective.

Knowledge: Current trends in the situation in which participants operate. Critical analysis of sources of information. Strengths & weaknesses of current approach.

Skills: Basic situational analysis from a security perspective.

Prerequisites: N/A

No. of Facilitators: 1

Technical Requirements: Large area of wall space, coloured paper in small squares or ovals, butcher paper, pins or blu-tack (to fix paper to wall).

Theoretical and Online Resources: Holistic Security Manual[30], Front Line Defenders Workbook on Security[31], and Protection International's Protection Manual for Human Rights Defenders[32]

Time: 90 minutes

Contributors: Sandra Ljubinkovic, Daniel Ó Cluanaigh, Ali Ravi, Nora Rehmer, Bobby Soriano, Peter Steudtner

Thanks to: Magdalena Freudenschuss, Craig Higson-Smith

Activity (15 minutes)

PEST(LE) analysis

Step 1. Preparation: On a large area of a wall, map out the 12 months of the last year (ideally with some butcher-block paper).

Step 2. Ask participants to write the most important events of the last 12 months that impact upon the context of their work on individual pieces of paper and plot them on the timeline. Ask participants to consider:

- political developments
- economic developments
- social developments
- technological developments.

Optionally, you may want to include:

30 https://tacticaltech.org/holistic-security
31 https://www.frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk
32 http://protectioninternational.org/wp-content/uploads/2012/04/Protection-Manual-3rd-Edition.pdf

- legal developments
- environmental developments.

Step 3. If you wish to add a layer of complexity, you may wish to allow participants to distinguish between:

- international developments
- national developments
- regional/local developments.

You can visually distinguish the different developments by using paper with different colours, or by tagging developments with a system of coloured dots. Give participants 10-15 minutes to carry out this exercise.

Discussion (10 minutes)

Consider the map of developments created by participants. Pose questions like:

- What trends can you observe from the past year in the different categories discussed (e.g., political, economic, social, and technological). What are the implications of these trends for your work?
- Are there any categories that we know less about? Why?
- What (or whom) are our sources of information for this? How trustworthy are they?
- What new sources of information do we need?
- Are there any events/trends/changes here that could have an impact on our security?

Input (15 minutes)

We often carry out situational analysis in our day-to-day lives, and make decisions for our security or well-being based on our analyses.

As HRDs, it helps to be a little more systematic about conducting situational analysis. Being more disciplined and organized helps us stay as aware as possible about our changing context, our **allies** and **adversaries,** and how our security may be impacted.

However, our ability conduct analysis depends to some extent on the availability of **sources of information** and their trustworthiness.

It may be difficult to find sources of information about certain topics, or we may not be in the habit of seeking out different sources of information. Therefore, it's a good idea to think critically about the sources we already rely on and actively seek new ones. We may want to consider:

- Talking to trusted friends and colleagues.
- Meetings with authorities, experts, diplomats and academics.
- Online tools such as Google Alerts.

- Regularly reading and analysing the local and international media.

Organising and conducting this analysis on a regular basis makes it easier to identify trends relative to your work. For example, the analysis could be updated on a weekly basis, or discussed as an agenda item during regular meetings.

Deepening (45 minutes)

Identifying and mapping trends

Groups from the same organisation or country

Step 1. If participants are from the same organisation or country, divide them into four groups (political, economic, social and technological). Each group is given a flipchart and markers to record key points. One person from each group should stay with the category throughout the activity, while the others will rotate at intervals.

Step 2. Ask participants to identify at least THREE developments within their given category in the last year which may have an impact (positive or negative) on their security and explain why.

Step 3. Give participants 15 minutes to get started, and then rotate the groups three times at intervals of 10 minutes. Participants may use the internet to search for information about anything they're not aware of.

Step 4. Make a gallery of the flipcharts. Ask some questions including: Did anyone discover **new sources of information** while carrying out the exercise?

Mixed groups

Option 1. If you have participants from several regions, or who share common issue areas, divide them into groups accordingly. Ask the groups to identify developments in each of the four categories (political, economic, social, and technological) for the **region** or **issue** their group has in common. Have them identify and explain 3 developments from any of the four analysis categories that they've identified.

Option 2. Alternatively, each participant can do this exercise individually and compare notes afterwards with another participant.

Afterwards: Make a gallery of the flipcharts. Ask some questions including: **Did anyone discover new sources of information while carrying out the exercise?**

Optional further deepening

If the group demonstrates relatively little knowledge of one particular area – a common example is the technological aspect – you may want to give them the task of researching developments in this area in their country or region and reporting back as a further deepening exercise.

Sample flipchart

Synthesis

Points to include in your synthesis are:

- Regular analysis of our environment will help us to identify opportunities and threats relevant to our work, our security and well-being.
- The strength of our analysis depends on the trustworthiness of our sources, so it helps to think critically about them.

Session 6: Vision and Actor Mapping

Objectives & Requirements

Attitudes: A clear vision for safely conducting their work as HRDs, informed by situational analysis.

Knowledge: Identification of the communities and individuals participants work with and for: allies, who can also protect them. Identification and mapping of actors who are opposed to the work of participants, including their resources and the modus operandi of opposition.

Skills: Basic actor mapping.

Prerequisites: Understanding of political, economic, social, technological contexts – ideally developed in Session 5: Situational Analysis.

No. of Facilitators: 1

Technical Requirements: Hand-out with the legend, flipchart paper for each participant OR a large sheet of butcher-block for the entire group, coloured sticky notes or paper, and markers.

Theoretical and Online Resources: Holistic Security Manual[33], Front Line Defenders Workbook on Security[34], and Protection International's Protection Manual for Human Rights Defenders[35]

Time: 70 minutes

Contributors: Sandra Ljubinkovic, Daniel Ó Cluanaigh, Ali Ravi, Nora Rehmer, Bobby Soriano and Peter Steudtner

Thanks to: Magdalena Freudenschuss and Craig Higson-Smith

Activity & Discussion (25 minutes)

Vision mapping

Within our socio-political contexts as human rights defenders, we have identified issues we consider unjust and want to change. It is useful to be clear and assert the change(s) we want to see in our society in order to think critically about how we go about achieving this change.

Groups from the same organisation

Step 1. On an area of wall space if possible, using a large sheet of butcher block paper, get participants to write the name of their organisation on a piece of coloured paper or sticky note and place it in the middle of the sheet. Draw an arrow from the middle to the right of the paper, leaving some space free at the end. Ask participants to brainstorm the goals they want to see achieved in their society, write them on sticky notes, and place them at the end of the arrow to represent the organisation's objectives.

33 https://tacticaltech.org/holistic-security
34 https://www.frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk
35 http://protectioninternational.org/wp-content/uploads/2012/04/Protection-Manual-3rd-Edition.pdf

Step 2. Ask the participants to think of the activities they carry out in order to achieve these goals. Write these below the name of the group or organisation in the middle of the sheet.

Step 3. Give everyone sticky notes or pieces of paper that are the same colour (e.g. green). Ask the participants to brainstorm (and write down on individual sheets) the names of other actors in society that support their organisation's work, or share their goals. Allow 10 minutes for this, then ask the groups to stick these actors on the left-hand side of the sheet.

Groups from different organisations

Step 1: Give each participant a sheet of flipchart paper, then ask them to write their own name (or that of their organisation) in the centre, with an arrow pointing right to represent their objectives. At the end of the arrow, participants should write (either on sticky notes or on the paper itself) the changes they wish to see in their society.

Step 2: In the centre of the page, underneath their name or that of their organisation, they should note the activities or projects they carry out in order to achieve these goals.

Step 3: On the left-hand side of their flipchart, participants should brainstorm to identify their allies (as above).

Input (20 minutes)

The next step in the exercise will be to carry out actor mapping, including our **allies**, but also our **adversaries** and the **neutral parties** ambivalent to our work. Carrying out actor mapping is important for a few reasons. From an analytical perspective, the mapping helps us to:

- Identify our allies and build security networks (we can return to our allies when it comes to building strategies and plans as well).
- Identify our adversaries, their resources and how they may try to stop our work.
- Identify opportunities for building acceptance of our work among neutral elements in society so that they become our allies.

The mapping exercise also helps us understand our own perceptions and to verify our assumptions. Furthermore, through the process of the mapping, we are able to consider more deeply the dynamics that connect different actors, and explore how these dynamics affect our security (whether positively or negatively).

Deepening (30 minutes)

Mapping allies, adversaries and neutral parties

Step 1. Hand out two more colours of either paper or sticky notes. Ask participants to brainstorm and write down **neutral parties** on one colour, and add them to the map around the centre of the page. Using the other colour, have them write down their **adversaries** and position them to the right of the page (between the organisation and its goals).

Ask participants to also consider whether adversaries are:

- intellectual authors of attacks (the people behind an attack)

- material authors of attacks (the people who committed the attack)

Step 2. Introduce the legend (overleaf) and give an example for each type of relationship.

Step 3. Give participants 10-15 minutes to map out the relationships between the adversaries, neutral parties and allies identified according to the legend.

Step 4: Questions for discussion with the group:

- Do any of your **activities** provoke a particularly strong reaction from adversaries? Should you prioritise these activities when making security plans?
- What are the **interests** of your adversaries? Why are they opposed to your work?
- Which **adversaries** do you consider to be the most dangerous? Why? What threats do they pose to HRDs/journalists?
- How can your **allies** help to protect you from your adversaries? What resources can they offer you (consider material resources, but also inspiration, hope, friendship, solidarity)?
- What opportunities are there to foster **acceptance** of your work among neutral parties or adversaries?
- What opportunities exist to **deter** attacks against using your relationships with powerful allies?

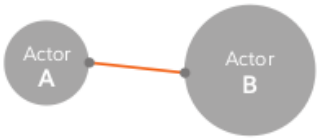
Synthesis

Points to draw out of this exercise in the closing part include:

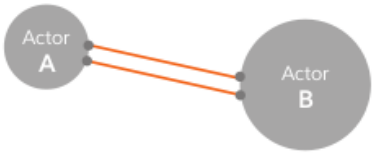
- Understanding the actors around us helps us to develop strategies which will open a space for us to continue our work, through protecting ourselves and building networks with our allies, or raising the costs (material, reputational or other) of attacks against us for adversaries.
- A key element we must now look towards, however, is information. Information about ourselves and our work is a valuable asset to our adversaries, and much of it now lives in digital devices, so we must consider how it is stored and moves between us, and which new actors we must add to our map.

Legend

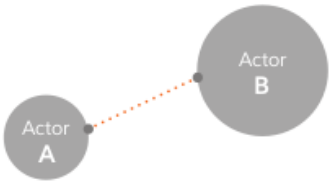
Different sized circles represent differences in power



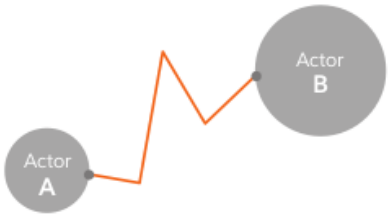
A solid line represents a close relationship
You can also 'break' the line (by crossing it in the middle) if there is a broken relationship



A double-line represents an alliance

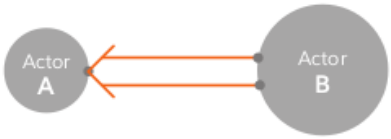


A dotted line represents a weak or unknown relationship

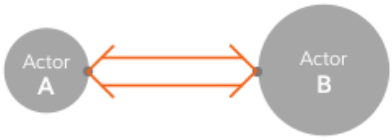


A jagged line represents conflict or a bad relationship

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

Session 7: Information Mapping (Part 1)

Objectives & Requirements

Attitudes: Understanding the importance of information as a valuable asset for ourselves, our allies and our adversaries. Information is a resource one can establish reasonable control over.

Knowledge: Information managed in the context of work given its unique sensitivity and characteristics. Add new actors to the actor map.

Skills: Basic information mapping.

Prerequisites: N/A

No. of Facilitators: 1

Technical Requirements: Flipchart, sticky notes, pens, markers, comic timing.

Theoretical and Online Resources: Holistic Security Manual (tacticaltech.org/holistic-security), Security in-a-Box (https://securityinabox.org/)

Time: 90 minutes

Contributors: Sandra Ljubinkovic, Daniel Ó Cluanaigh, Ali Ravi, Nora Rehmer, Bobby Soriano and Peter Steudtner.

Thanks to: Magdalena Freudenschuss, Craig Higson-Smith and Samir Nassar. Contains material adapted from Level-Up (https://www.level-up.cc/).

Activity (30 minutes)

Mapping information at rest

Tell participants that the exercise will be to conduct an information mapping activity to get a sense of where our important information actually is.

Step 1. Start by asking participants to list the different places where our information is stored. If no suggestions are forthcoming, prompt participants with some of the obvious locations:

- computer hard drive
- USB flash drives
- external hard drive
- cellphone
- CDs, DVDs (and BDs)
- email inbox
- 'the cloud' – Dropbox, Google Drive, SkyDrive, etc.

- physical copies (or 'hard copies') in the office/at home
- multimedia: video tapes, audio recordings, photographs, etc.

Step 2. Add these titles to a flipchart or whiteboard and construct the matrix around them if you have not already done so (see below).

Step 3. Ask participants what type of information or data they have in each of these places. For example:

- emails
- contact details, such as a member database
- reports/research
- accounts/spreadsheets
- videos
- images
- private messages on Facebook, etc.

Step 4. To encourage participant interaction, write one example on a sticky note and place it in the appropriate box in the matrix. Then, ask whether there is another copy (backup) of this data somewhere else. If there is, you can use another sticky note (preferably one of a different colour) and put it wherever they keep the duplicate/backup. You can use this moment to highlight the difference between master copies and duplicates.

Repeat this process with another example, hopefully provided by a participant.

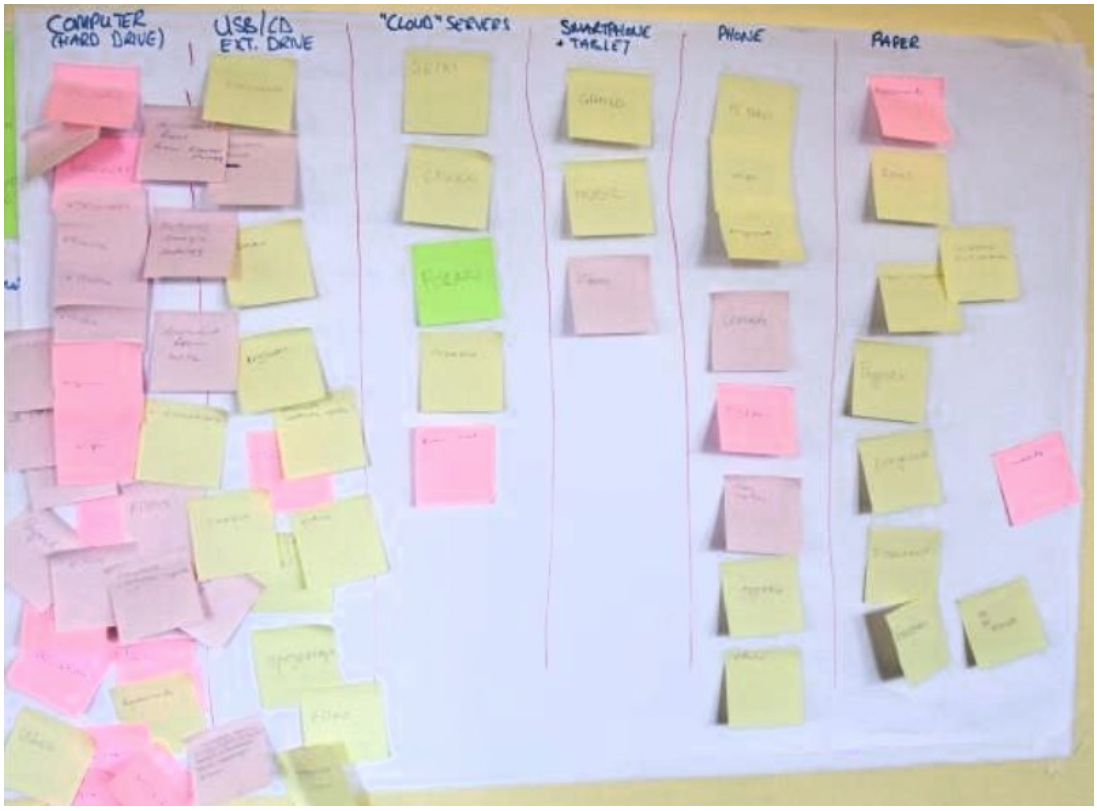
Optional step: Include a "sensitive / non-sensitive" axis. Looking at the two examples, introduce the axis representing sensitivity. The higher on the chart, the more sensitive the data. Place the two sticky notes on this axis representing their relative sensitivity.

Step 5. Give participants sticky notes and ask them to consider the different data they have on each of the devices identified. Emphasise that they should write **one** thing per sticky note.

Participants can define the level of detail, depending on the level of trust in the group. However they should be detailed enough to distinguish between different levels of sensitivity, e.g. “interviews” vs. “interviews with victims”.

Step 6. Ask participants to place their sticky notes on the information map.

Sample information map



Discussion (5 minutes)

Ask participants for any observations they have about the information map. Questions might include:

- Is there a large dependence on one device or another?
- Is much of the information online? If so, on whose property (or whose server) is it being stored?

Input (15 minutes)

Threats to information at rest

Step 1. This is just the beginning of an information map. It would be almost impossible to map all the data around us, but we can focus on the things we consider most important and sensitive.

Ask participants: Have they ever experienced *data loss*? If so, how did it happen?

Step 2. [Dramatically] remove all the sticky notes from one column in the map (such as the computer hard-drive) and throw, brush, or knock them on the floor suddenly. Explain that this is essentially what happens when we experience data loss – suddenly the copies in other locations are all we are left with.

There are many things that can cause data loss. It is not a question of if, but when it happens. How can we protect ourselves from that shocking moment when we realize we've lost something valuable or even irreplaceable?

Step 3. Remove one sticky note from another column, such as mobile phone or email. Ask participants, what happens if I can access this piece of information? If I can just take it and read it? How would you protect this data?

As you go through the above, write the primary threats to information at rest on a flipchart:

- data loss
- malware infection
- unauthorised access and surveillance

And the basic ways of protecting it:

- backups
- good general 'digital hygiene' practices
- anti-virus
- strong passwords
- secure deletion
- encryption.

Deepening (30 minutes)

Written information map

Give participants an information map printout (see Appendix), and give them 20 minutes to begin filling it in. Group participants according to whatever is most useful. If they are from the same organisation, perhaps according to their organisational structure. If they are a mixed group of participants, then have them join in small groups according to organisation, issue or other affiliation. At the end of the exercise, ask participants for reflections on the process.

Example information map

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

Synthesis

Points to draw out during the synthesis include:

- Information is one of our most important assets. It often has a lot to do with our allies, and is of great interest to our adversaries, who want to gather as much information about us as possible.
- Information is not only at risk when it is at rest, but also as it moves through electronic channels (as explored in the next exercise).

Session 8: Information Mapping (Part 2)

Objectives & Requirements

Attitudes: Critical awareness of threats to sensitive information as it is transferred digitally ('data in motion').

Knowledge: Understanding of how data travels electronically and the points at which it can be subjected to surveillance. Adding important actors including internet service providers, online service providers, etc., to their actor map . Basic threats to information in motion and a framework for responses.

Skills: Basic information mapping.

Prerequisites: N/A

No. of Facilitators: 1

Technical Requirements: flipchart/whiteboard, markers, envelopes, postcards/small sheets of paper, pens, cipher (see Appendix) **or** two small boxes with locks and keys.

Theoretical and Online Resources: Holistic Security Manual (tacticaltech.org/holistic-security), Security in-a-Box (https://securityinabox.org/)

Time: 115+ minutes

Contributors: Sandra Ljubinkovic, Daniel Ó Cluanaigh, Ali Ravi, Nora Rehmer, Bobby Soriano and Peter Steudtner

Thanks to: Magdalena Freudenschuss, Craig Higson-Smith and Samir Nassar. Contains material adapted from Level-Up (https://www.level-up.cc/).

Activity & Discussion (30-45 minutes)

How the internet works – starring *Romeo and Juliet*.

Note: There are a few adjustable elements to this activity that should be altered depending on the number of participants and the time available.

Step 1. Get participants to sit in a semi-circle facing the flipchart. Designate the people at either end of the semi-circle a 'Romeo' and a 'Juliet' (can also be "Romeo and Romeo", "Juliet and Juliet", or any other combination).

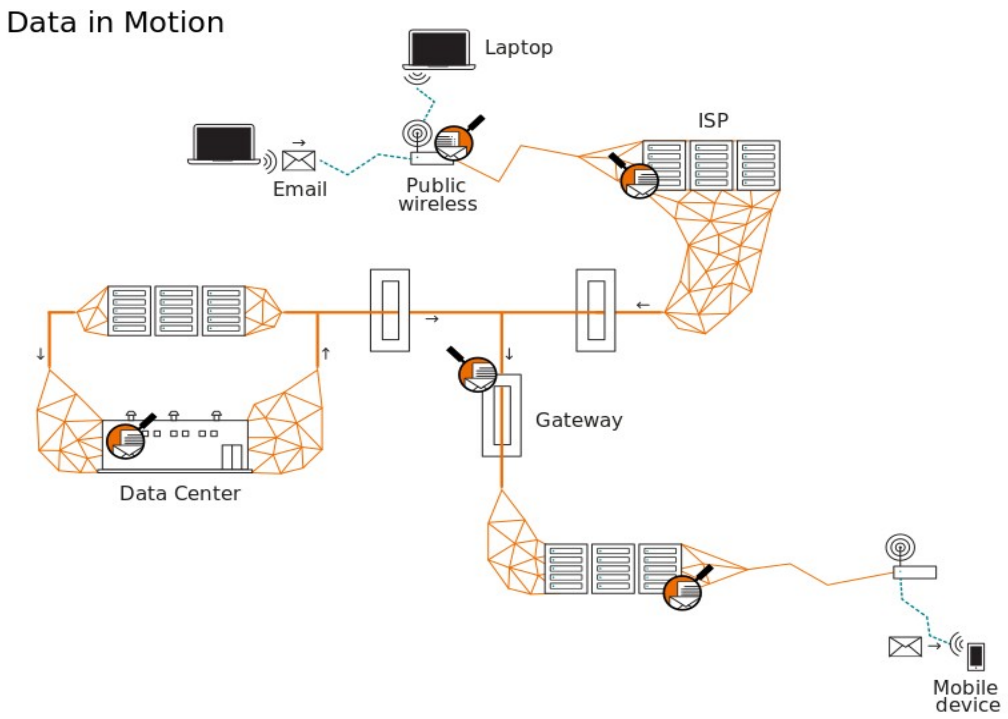
Step 2. Instruct Romeo to write a message to Juliet. Romeo and Juliet will communicate, but since there is no internet, they depend on us to help them.

Step 3. Once Romeo has written the first message, have him pass it around the semi-circle until it reaches Juliet. Ask each person what she or he can read of the message. After the email has been delivered and read by Juliet, ask participants what they were able to learn from the messages as they 'routed' it to Juliet.

Step 4. Information transferred using the internet (in this example, an e-mail) passes through a number of locations as it is transferred electronically. **In the case of Romeo's email to Juliet, it would pass through several points**, which the participants will represent.

Give participants a sheet indicating their role (in order as they move **away** from both Romeo and Juliet towards the 'centre' of the semi-circle). Depending on the number of participants, you may need to adjust which roles you hand out.

- **The computer** of the sender (or recipient) of the message (i.e. Romeo was the sender in the first message sent, and Juliet was the recipient).
- The **router** in the building or area where Romeo connects to the internet
- The **Internet Service Provider of the sender (and recipient)**, who sometimes owns the router. ISPs provide access to the internet, and are usually a large companies that must comply with the laws of the country.
- The **National Gateway(s)** are part of the telecommunication infrastructure of the country, where optical cables enter the physical territory of the country. It is often controlled by the state, or may be operated by a private company on behalf of the state (such as an ISP). Data may pass through several countries, and multiple ISPs and National Gateways as it travels to the servers of the recipient's online service (in our email example). Eventually the email will arrive at the Gateway of the country in which the sender's email service provider is based (if different from the country he sent the email from). When it is routed from there to the recipient's email service provider, it may cross multiple ISPs and National Gateways again.
- The **ISP of the email provider** (e.g. Yahoo!, in the United States)
- The **servers of the service provider**.



Step 5. To illustrate this, have Juliet write a postcard response to Romeo, routing the messages through the various points of the internet. Explain each point as the message is routed. (If it is helpful, you can give the scenario more detail, using a country, ISPs, and providers that are familiar to participants.)

Explain that when Juliet checks her email, the mail will pass through a combination of the above again before arriving at her ISP, her router and her computer. Then, when Juliet replies to Romeo, the email data will pass through a similar route to reach the computer where Romeo reads her response.

Step 6. Encryption of data in motion:

HTTP traffic is like a postcard

Use this first round of communication between Romeo and Juliet to explain that when our communications are travel they are just like a postcard. And, like a postcard, this can be read at every point along the way. In this email scenario, we can call this traffic HTTP traffic – it travels in the open for everyone to read.

HTTPS traffic is like a letter in an envelope

Ask participants what they could do to protect the message on the postcard. Elicit the idea of putting it into an envelope if needed. Provide an envelope to the person representing an email service provider (e.g. Yahoo!).

Step 7. In this case, Romeo and Juliet can only utilize HTTPS if their email service provider implements it, so the envelope is provided the email service provider (Yahoo!). Romeo or Juliet must **ask for the envelope**, write another message to put inside the envelope, then write the 'address' for the recipient on it. (At this point, you should decide whether or not Romeo's email service provider is **also** implementing HTTPS.) Explain that HTTPS is a type of encryption—it encrypts data in motion from one server to another, so that points in between cannot read the content of a message.

Step 8. Have Juliet respond to Romeo using HTTPS provided by her email service provider. Ask participants to note what information they can capture as the message is 'routed' through them. After it is delivered and opened, ask participants what they could observe about the message.

Building on their responses, make the following points:

- In order for the message to benefit from HTTPS from sender to recipient, the email service providers of both Romeo and Juliet need to implement HTTPS. If only Juliet's email service provider uses HTTPS, it means the message can be observed by participants closer to Romeo.
- Provided that both email service providers implement HTTPS, **only the email service providers can read the message** since they provided the envelope. They can also copy and share this content.
- Everyone else in the chain can only read the address and the names of the sender and recipient. This is **metadata**.
- **Metadata** is still important and widely used for surveillance. Sadly, we can't only focus on the sensitivity of our digital **content** (in this case, the messages). This is because metadata

is often 'enough' for adversaries (both state and non-state actors) to discern a great deal about our activities.

Since this activity had a lot of information that may be new for participants, offer to answer any questions they may have about the activity. You may also want during this activity to draw a diagram of "How the internet works" on a flipchart or whiteboard. See Appendix for a sample flipchart drawing.

Optional extra step: Metadata: While in real life we send postcards detailing physical addresses, devices also have addresses (and additional details) they use to 'route' data around the internet. These are called **IP addresses**. In this case, the 'address' used to send and receive emails gives a crucial detail to everyone who can see it in order to route a message properly to the intended recipient. Everyone can also see the IP address from where the message was sent.

IP addresses usually refer to concrete physical addresses too. Demonstrate this to the group using https://whatismyipaddress.com.

Input (45 minutes)

Option 1: Sending messages with end-to-end encryption using a lockbox

Step 1. Imagine that one day a magical 'gnome' (the facilitator) appears to Juliet and says to her:

"Juliet! Do you want Romeo to send you a note so that no one along the way can tell what it is? Then you should give him this, your very own open lockbox. This is a magical lockbox."

Step 2. Hand Juliet the open box.

Your lockbox is 'magical' because:

- You have as many of the same lockbox as you want.
- You can give it to whomever you want to be able send you confidential messages.
- Once they put their message in your lockbox and send it to you, another lockbox is magically available for them to use.
- Once they close and lock your lockbox, only its **private key** can open it.

Step 3. Hand Juliet the key.

- This is your **private key**. **Only you** have this key. It is yours, and it is private.
- Keep your private key **very safe**.
- **Don't lose or share** your private key. It will always open this lockbox and all of its copies.
- If you lose this private key, you will **never again be able to open the lockboxes** associated with it.

Optional metaphor for self-authentication via password:

The private key will imprint itself on you the first time, with your kiss. Thereafter it will only work after you kiss it to tell it that it is you who are using it and no one else. From this point on, the key will only work with your kiss.

Step 4. (Concept checking) Ask participants:

- What does Romeo need in order to send Juliet a message? [Her lockbox]
- Can Juliet send him a private message back? [Not yet]

Step 5. In order for both sides to be able to communicate privately, they *both* need a lockbox and they *both* need a key. The gnome repeats the same process with Romeo.

Step 6. Romeo and Juliet now have everything they need in order to communicate securely. All they need to do is exchange lockboxes! How can they do this?

- in person
- through the postal system (as during the previous activity)

Step 7. Have Romeo and Juliet exchange lockboxes.

Step 8. Have Juliet send Romeo a message in his lockbox. No one in the chain can read the message, but as before they can see the address on the outside of the box (metadata). You may want to use a sticky note or gift tag to attach the address to the lockbox.

This process is how a type of powerful email encryption called GPG works. Each of us has a public 'lockbox' that we send to others, and a private key which is password-protected and which we maintain for ourselves and share with nobody. In order to communicate securely, we exchange our public lockboxes (also known as 'public keys'). After that, we can use certain computer programs to encrypt and send messages.

However, when a 'lockbox' (encrypted message) goes through the postal system, the different points that route the message may be able to tell that it is an encrypted 'lockbox' message. If both mail providers have HTTPS, then only they will be able to tell that it's a 'lockbox' message. But if one or both of the email providers **don't** use HTTPS, then other points routing the message will also be able to tell that it's a 'lockbox' message. Keep this in mind if you are concerned about drawing attention to your messages, by only using a trusted email service provider that has HTTPS, but also be thoughtful about the safety of the recipient of a message as well.

Option 2: Sending messages using a cipher

Step 1. Give Romeo and Juliet a copy of the cipher text key (see Appendix) and allow them to write another message using the cipher. Send it through the same system again.

Step 2. Ask each participant routing the message how much they are able to understand.

In this case, even an email service provider will not be able to understand the content of the message, since it is encoded.

Romeo and Juliet just managed to keep their communication secret through a process called **end-to-end encryption**. Show the cipher to the participants. Since both Romeo and Juliet had the cipher, they are the only ones able to decode the message. However, this is suspicious! (As the facilitator, you may want to play the role of the intelligence agency and ask the email provider for a copy of the message.)

Circumvention and anonymity

We can circumvent the system of IP addresses that facilitate censorship and online tracking through using software such as a **VPN** or **Tor**. A VPN is less effective at anonymising your traffic,

although it is less suspicious. Tor is more effective at anonymising, but may be more suspicious.

Deepening (30 minutes)

Written information map – Information in motion

Summarise the threats to sensitive information in motion after the exercise. Also summarise potential mitigation tactics and their advantages and drawbacks. You may want to create a table such as the below to help participants navigate all the information you've covered thus far:

	HTTP	HTTPS	End-to-end Encryption	TOR
Content protected from ISP (and whomever they share it with)	No	Yes	Yes	Yes
Content protected from website/service owners (and whomever they share it with	No	No	Yes	No
Metadata protected?	No	No	No	IP Changed
Suspicious?	Depends on content	No	Potentially	Potentially

Introduce the information map for information in motion, explaining each of its parts. Ask participants to fill out the map for information in motion (Appendix) for 15 minutes and share reflections.

Synthesis (10 minutes)

Ask participants what they've learned during this session. Was there anything new? Anything different than what they knew before? What did they discover that was useful? What questions do they still have?

Expanding the actor map

Ask participants to return to their **actor maps** and add any important new actors according to the map of how the internet works.

Example information map

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

Session 9: Security Indicators, Sharing and Analysis

Objectives & Requirements

Attitudes: Appreciation of situational security indicators and the need for sharing them. Openness and appreciation of colleagues and friends sharing indicators

Knowledge: Definition of security indicators. Best practices regarding sharing and analysis of security indicators. Exploration of security indicators by participants in their current situation.

Skills: Analysis of security indicators.

Prerequisites: Output from the Situational Analysis exercise in Session 5.

No. of Facilitators: 1

Technical Requirements: flipchart

Theoretical and Online Resources: Holistic Security Manual[36], Front Line Defenders Workbook on Security[37], and Protection International's Protection Manual for Human Rights Defenders[38]

Time: 75 minutes

Contributors: Sandra Ljubinkovic, Daniel Ó Cluanaigh, Ali Ravi, Nora Rehmer, Bobby Soriano and Peter Steudtner.

Thanks to: Magdalena Freudenschuss, Craig Higson-Smith and Samir Nassar. Contains material adapted from Front Line Defenders' Workbook on Security for Human Rights Defenders.

Activity (10 minutes)

Give participants a scenario (or series of scenarios) where a HRD identifies security indicators and makes decisions that keep them safer.

Show participants the scenario(s) and give them 5 minutes to read it. Here is an example taken from Front Line Defenders' *Workbook on Security*:

> "We noticed taxis started parking outside our office. Staff would often take these taxis rather than going to the nearest taxi rank as usual. The taxi drivers started conversations with the passengers, asking what they had been doing that day.
>
> Our organisation regularly met with other organisations to discuss their work and security issues. At the next meeting, we mentioned this security incident. Members of the other organisations present then realised that taxis had also started parking outside their offices too.
>
> We concluded that the authorities were either using taxi drivers to collect information on us, or had planted security personnel as taxi drivers. Our organisations then decided that the safest response would be to pretend we had not noticed, but we warned the staff not to

36 https://tacticaltech.org/holistic-security
37 https://www.frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk
38 http://protectioninternational.org/wp-content/uploads/2012/04/Protection-Manual-3rd-Edition.pdf

say anything about their work in the taxis but instead to chat about harmless issues."

HRD, Americas

Discussion (10 minutes)

Ask participants:

- What were the best practices used by the HRDs?
- Finding taxis outside the office suspicious may seem like paranoia. How did they 'check' whether they were paranoid?
- In your opinion, did they make the right decision to continue using the taxis?
- Do you have any similar experiences to share?

What the HRDs have done in this scenario is a great example of noting, sharing and analysing security indicators, in order to make decisions about their security.

Input (15 minutes)

Security indicators are anything out of the ordinary that we notice which may have an effect on our security. They are sometimes called security **incidents**, although they do not have to refer to concrete events.

We can identify security indicators at various different moments in our daily life and work. Examples of these include:

- receiving a letter from the authorities about an impending search of the office
- someone taking a picture of you in a public place
- 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.

We may be quite used to perceiving security indicators in our environments, but we can also look for them in our physical and emotional experiences, which may indicate that we're close to burning ourselves out. Consider what kind of physical sensations, thoughts or mental states might be indicators of stress, fatigue, or burnout.

The behaviour of our electronic devices can also change and indicate that they may be compromised. Consider what indicators might alert us to:

- a virus infection
- someone breaking into our email accounts.

The most important thing to do with security indicators is to **record them** and **share them**. Analysing them together with others is a good way to **check our perceptions and jointly decide if a response is required**.

If it's useful, introduce an example format for **recording security indicators** (see Appendix).

Remember: Security indicators can also be **positive** indicators, demonstrating that we are doing things right and taking effective security measures. For example:

- noting that authorities begin to act in protection of other HRDs in your region more effectively
- decreasing crime rates in an area where you work
- noting that your stress levels are lower and you are more alert than before to your security situation.

Deepening (30 minutes)

Recording and sharing security indicators

Process for groups from the same organisation:

Step 1. Participants return to the map of the trends in their context over the previous 12 months (Session 5: Situational Analysis) and add any attacks or other security-related events that have affected them during this period.

Step 2. Participants organise into small groups either per incident identified, according to their area of work, or other affinities within the organisation.

Step 3. Focussing on a given security event they have experienced, participants should share any security indicators that they can remember which may have alerted them to the event prior to it occurring. If desired, they can share and record the events in writing. See Appendix for an example format. Remind participants of the definition of security indicators.

Step 4. Groups report back to the larger group on the security indicators they identified.

Safe spaces for sharing

Sharing security indicators can be a sensitive moment, as it also means that we sometimes share mistakes we have made while we were under pressure, not paying attention, tired, stressed or confused. In order for us to feel able to share, a safe and trusting environment must be created where people are not blamed for things they are perceived to have not done correctly or not been aware of. Rather, they should be appreciated for sharing indicators that help the collective make informed decisions about their security going forward. If necessary, you may want to introduce tools for non-violent communication in order to facilitate sharing of security indicators. See the section on non-violent communication in the Holistic Security Manual.[39]

Process for mixed groups:

Step 1. Divide the group into pairs. Tell participants they are going to be security consultants. They will interview one another about a previous attack or security event that they have experienced, and try to help each another identify the security indicator(s) that alerted them (or could have alerted them) to something being wrong.

39 https://holistic-security.tacticaltech.org/chapters/prepare/1-5-communicating-about-threats-in-teams-and-organisations

Step 2. Each participant takes 5-10 minutes to explain the event to his or her partner. Their partner can then ask them questions or simply listen for 10 further minutes about the security indicators around the event. Together, they fill in a register of security indicators, and then swap roles and repeat the process.

Further reflection

Discuss with participants:

- What spaces have they made in the past for sharing and analysing security indicators?
- How can they integrate space for this into their current workflow? Could it be on the agenda at regular meetings? How will they integrate space for sharing and analysing indicators into particular activities?

Ask participants to reflect on their own organisation. What would be the best way to record **security indicators**, analyse them and take action where necessary? For example:

- Someone designated to keep a security indicators record book.
- Someone tasked with highlighting need for joint analysis of security indicators.
- Establishing an effective and realistic decision-making process to decide if reaction to security indicators is necessary. (For example: Who should be part of this process? How are these decisions and their implementation documented for organisational learning? Etc.)

This proposal could go into the planning/moving forward session at the end of the training.

Synthesis

Security indicators are very useful in alerting us to potential threats to our security. If they are properly noted, shared, and analysed, they can help us take preventive action.

Encourage participants to share best practices and identify an organisational way for dealing with security indicators. Consider:

- Where are indicators recorded?
- How are they shared and with whom?
- Who is responsible for analysing them and decides upon a reaction if necessary?

While we have a physiological instinct for noting some indicators, others are less clear and we need to look for them more actively as a part of our routine.

Since overworking and stress can challenge our memory, it's a good idea to maintain a written record of security indicators that facilitates the sharing and the maintenance of historical 'memory' in our organisations.

Session 10: Threat Analysis

In this exercise, we walk participants through a process of identifying and prioritising concrete potential threats to their work and their well-being in the context of their activities, for which they can later prepare.

Objectives & Requirements

Attitudes: Taking the time to analyse activities in light of potential threats helps us to prepare more effectively for them.

Knowledge: Threats related to activities. Impact and likelihood as elements of risk.

Skills: Basic threat analysis related to their activities.

Prerequisites: It is best if this activity follows a thorough context analysis (Session 5) and vision and actor mapping (Session 6).

No. of Facilitators: 1

Technical Requirements: flipchart/butcher paper, markers, sticky notes, hand outs (optional)

Theoretical and Online Resources: Holistic Security Manual[40], Front Line Defenders Workbook on Security[41], and Protection International's Protection Manual for Human Rights Defenders[42]

Time: 75-90 minutes

Contributors: Sandra Ljubinkovic, Daniel Ó Cluanaigh, Ali Ravi, Nora Rehmer, Bobby Soriano, Peter Steudtner.

Thanks to: Magdalena Freudenschuss, Craig Higson-Smith and Samir Nassar.

Activity & Discussion (25 minutes)

Threat brainstorming

For groups from the same organisation

Step 1. Using a large sheet of butcher paper on the wall, participants map out the main **activities or areas of work carried out by the organisation**, which were identified in the vision and actor mapping exercises in Session 6. If the organisation has an office, be sure to include the daily running of the office as an activity here.

Step 2. Introduce the exercise. Participants will brainstorm threats to themselves and their well-being as they relate to each activity. On a flipchart, write the definition of what a threat is as a reminder:

40 https://tacticaltech.org/holistic-security
41 https://www.frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk
42 http://protectioninternational.org/wp-content/uploads/2012/04/Protection-Manual-3rd-Edition.pdf

A threat is any potential event that could cause harm to ourselves or our work.

Step 3. Divide participants into groups according to each activity. It may be according to activities that they actually work on, or divided randomly. Each group uses sticky notes to brainstorm threats they associate with each of the activities.

Remind participants to consider:

- Their situational analysis of the political, economic, social and technological trends.
- The actors who oppose their work and their **modus operandi** by trying to close their work space.
- Any security indicators they have experienced that might alert them to likely threats.
- Threats to their health and well-being, as well as threats to their sensitive information.
- Threats do not have to be political in nature. They can also arise from common delinquent violence and environmental factors (e.g. malaria or dengue when travelling,, acts of nature, etc.).

Sample instructions:

For each of your activities or areas of work, consider all the potential threats to yourself, your organisation and your 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.

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

Observe any patterns that emerge in the threats you identified: Do they relate primarily to certain activities of yours, or originate from certain adversaries? 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.

For mixed groups

Participants are given blank flipcharts or hand outs and carry out the exercise alone (according to the instructions above). After completing their brainstorm, they then share their findings with a partner.

Input (15 minutes)

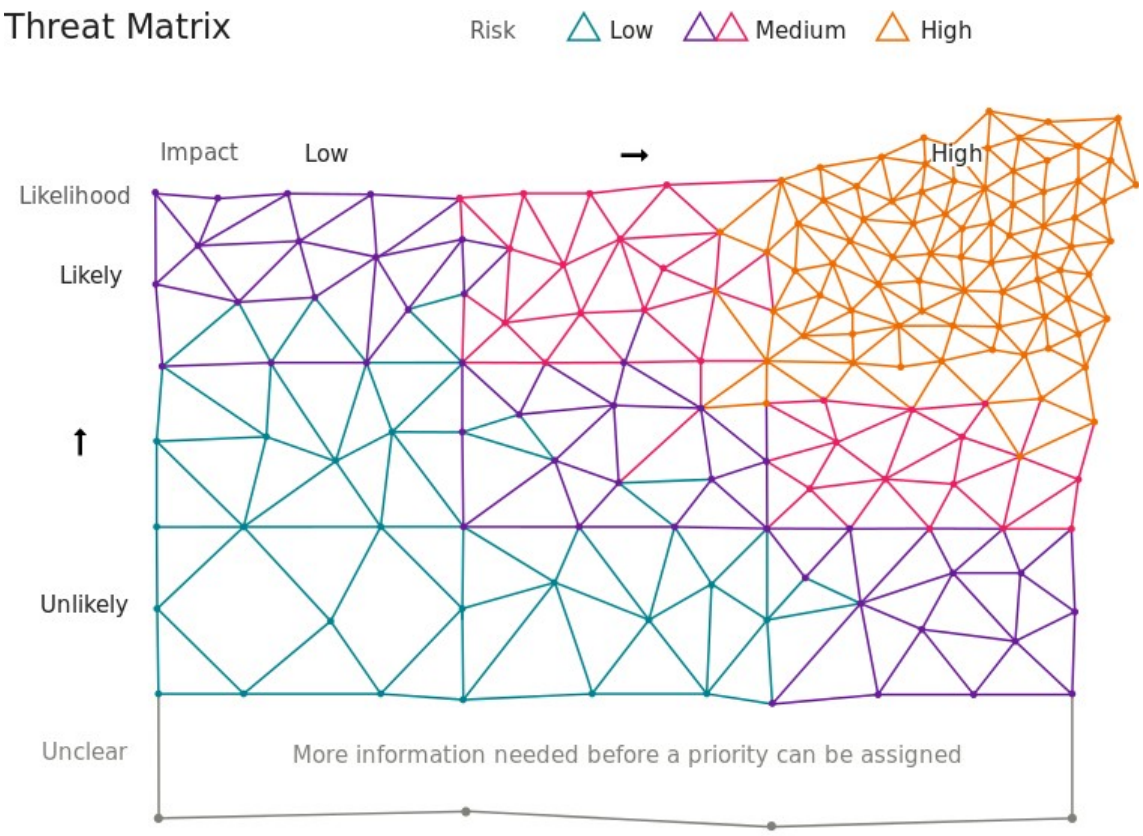
Prioritising threats

Step 1. There may be many threats we can imagine happening in the course of our work. This can be overwhelming. However, at some point we have to prioritise the threats we face in order to take practical steps to move forward.

One method that helps prioritising threats is to distinguish them according to their relative

probability (or **likelihood)** and **impact**. These are two elements of a **risk analysis.**

Step 2. Present the threat matrix as demonstrative of this. You can create a simplified version of the one below by simply plotting two axis representing likelihood and impact and measuring from low to high.



Deepening (30 minutes)

The threat matrix

For groups from the same organisation

Step 1. Ask the groups to create a threat matrix for each of the activities they identified in the previous exercise (e.g., the activities they regularly carry out in defence of human rights). Give each group sticky notes and pens.

Step 2. Give the groups 15-25 minutes. On each matrix, they can place the threats according to their perceived likelihood and impact. In groups, they can discuss their perceptions regarding the likelihood and impact of each threat. Emphasise that this needs to be done respectfully and that each member of the group should be given space to speak.

For mixed groups

Step 1. Each participant creates a threat matrix on a flipchart and has 15-25 minutes to complete it.

Step 2. They then pair up and present and discuss their threat matrix with their partner, asking questions if necessary to check their perceptions. The facilitator should move from pair to pair, seeing if there is any confusion and helping out where necessary.

Not Knowing: For this exercise, it's good to openly recognise that it can be very difficult to know where to put some threats. In many trainings, participants feel under pressure during this exercise, as if there is a 'right' or 'wrong' answer. Our perceptions are challenged, on the one hand, by stress and tiredness and other factors. On the other hand, they are also challenged by a lack of publicly available information about certain threats (such as electronic surveillance).

Ensure that participants have a chance to explain to one another why they feel that a particular threat has a corresponding likelihood or impact, and promote calm discussion and analysis of it, based (if possible) on the notion of security indicators. This exercise is best done with plenty of time and no sense of rush, as it can also be a rather difficult moment to realise again that certain threats—particularly existential threats—are in fact a reality for the HRDs in the room.

Step 3. Explain that this output will be used as the basis for the following sessions, where we will see how our existing strategies, plans and tactics match up to these threats, and make plans to build and strengthen them.

Optional Deepening/Homework

Specific threat analysis

Especially for organisations or groups who have plenty of energy and/or are rather cerebral, you may want to share the **threat inventory** (below) as a further deepening that allows participants to analyse a particular threat and its consequences in depth.

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				

If there is not enough energy in the room for this, simply present the format on a flipchart and share it with participants for later use.[43]

Synthesis

Points to draw out of this exercise in the closing part include:

- The threats that we have identified can be used as entry points to building strategies, plans and tactics for us to keep working and be safe and well.
- In our strategic planning, it's important to consider the potential threats that may arise from our activities. In the first instance, they help us decide whether or not the activities are a good idea, and if so, how to carry them out more safely.
- This looks like a scientific, objective operation – but really it's about perceptions, which can be challenged when we're under stress, or when we're talking about threats that are mediated through a digital medium (such as electronic surveillance). In this case, we should check our perceptions with trusted friends and colleagues, or try to find more information.

43 https://holistic-security.tacticaltech.org/chapters/explore/2-8-identifying-and-analysing-threats

Session 11: Security Planning Essentials

Note: Security plans and strategies could itself be a workshop of at least one full day. This session is more of an introduction, overview and summary of some of the main points, but in itself probably not sufficient for a mixed group or organisation to consider the topic 'covered'.

Objectives & Requirements

Attitudes: Plans and strategies are useful for organising and grounding our security practices.

Knowledge: Essential elements of a security strategy and plan. Capacities needed to be built.

Skills: Developing a basic security plan.

Prerequisites: An analysis of the prioritised threats participants face while carrying out their work (Session 10).

No. of Facilitators: 1

Technical Requirements: N/A

Theoretical and Online Resources: Holistic Security Manual[44], Front Line Defenders Workbook on Security[45], and Protection International's Protection Manual for Human Rights Defenders[46]

Time: 90-110 minutes

Contributors: Sandra Ljubinkovic, Daniel Ó Cluanaigh, Ali Ravi, Nora Rehmer, Bobby Soriano, Peter Steudtner

Thanks to: Magdalena Freudenschuss, Craig Higson-Smith; Samir Nassar

Input & Activity (40 minutes)

Basic security plan

Step 1. Having analysed the threats faced in our work, ask participants to make a simple security plan to correspond to one of the activities in their work (ideally, one which was used as a basis for the threat analysis exercise), and present it to another participant.

The **objective of the activity** and the **threats associated with it** are the basic starting point for planning.

For each threat identified, it's useful to consider two corresponding things:

- **Existing security practices** and **capacities**. These include well-being, attitudes, knowledge, skills and resources that we can access to help keep us safe from a particular threat.
- **Gaps in our existing practices** and **vulnerabilities**. These include the attitudes, knowledge,

44 https://tacticaltech.org/holistic-security
45 https://www.frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk
46 http://protectioninternational.org/wp-content/uploads/2012/04/Protection-Manual-3rd-Edition.pdf

skills, resources, and well-being (or lack thereof) that make us more susceptible to a threat.

Step 2. Security plans can be written or unwritten—it depends largely on the culture of the group or organisation.

However, it's good to keep in mind that each plan should include the following **as a minimum**:

- the objective of the activity
- the threats identified
- preventative actions and resources
- response and emergency actions and resources
  - including **when** do you define a situation as an emergency?
- communication and devices
- well-being and self-care

Using this as a guide, create a security plan for one activity you carry out in your work. Use the threats you identified as the basis for the tactics and tools you will use. It doesn't all have to be new - include also your already existing strategies and capacities.

Step 3. Give participants 20 minutes to draft a plan, and then 15 minutes to present their plan to a fellow participant.

Variations for organisations or mixed groups

For organisations, participants can work in small groups according to area of work or another organising principle. For mixed groups, participants should work individually at first on a plan relative to their work.

Discussion (10 minutes)

Pose the following questions to the group:

- How do you know the tactics you are using are the right ones?
- Where does the plan fall short? What are things you cannot yet protect yourself against?
- Are there any new skills, tools, or tactics you will need to learn in order to implement this plan?

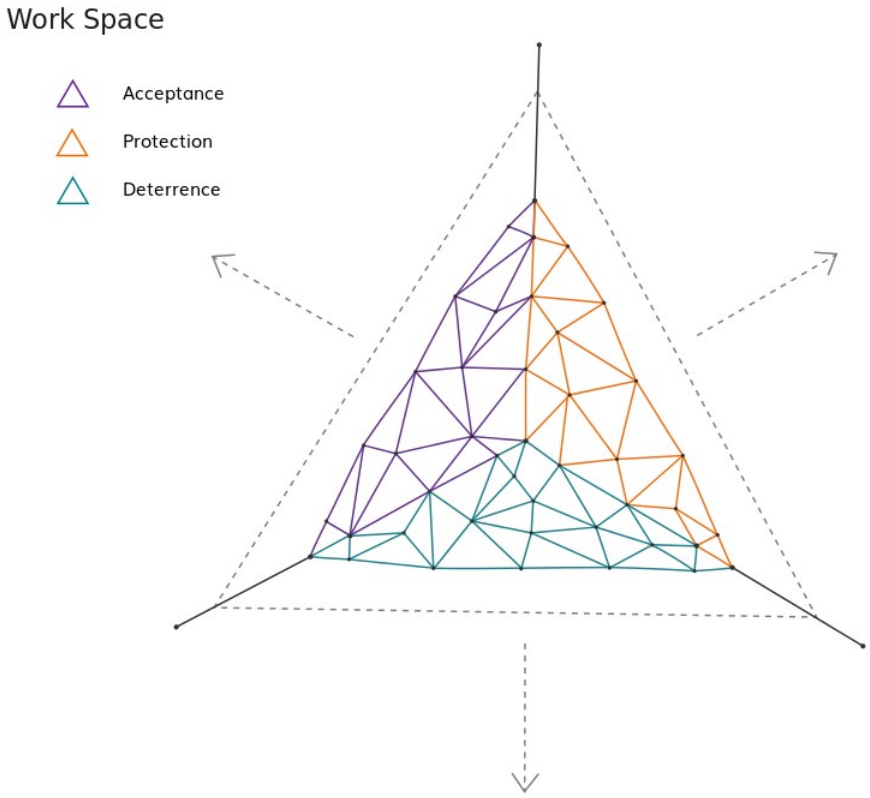
Input/Discussion (20 minutes)

Security strategies

We've practised making a plan for a single human rights activity. But it's a good idea to have an overall strategy rather than to just plan for single events. If we have a strategy, then we can use it as a basis for drawing up plans as our work demands them, and according to our own rhythm and style of working.

Introduce the ideas of **acceptance**, **deterrence** and **protection** strategies while drawing and explaining one at a time, using the diagram example below, which visualises them as ways of opening the socio-political space for your work.

- **Acceptance:** Building support for our human rights work among the actors around us, including our 'opponents'.
  - What are examples of ways you already build acceptance of your work?
- **Deterrence:** Raising the political cost of attacks against us, so that our opponents decide not to carry them out.
  - What are examples of ways you already deter attacks against you?
- **Protection or self-defence:** Building our own strengths so that our opponents can't attack us so easily.
  - What are ways you already act to protect yourself?



The tactics you use in your security plan will usually fall into at least one (maybe more) of these categories. But we don't just plan for high-risk events or moments—we can carry out these activities on a day-to-day basis and build them into our work, or the work of our organisation.

A security strategy may comprise a number of different plans, and each plan will mean using various tools and tactics that correspond to the threats we have identified.

These tools and tactics will need to be updated as time goes on and threats around us change. Therefore, we may have to learn new things and also spend time and money on building new capacities.

Deepening (20 minutes)

New skills, tactics and resources required

Step 1. Draw a matrix like the one below on a flipchart or whiteboard and ask participants to reproduce it.

Threats	New Capacities	Resources Needed

Step 2. Give participants 15 minutes to consider the threats they have identified, the new capacities they need to build, and in this respect, the resources they need in order to build them.

Synthesis

Points to draw out in the synthesis include:

- Making security plans and agreements of some kind helps us to have at least some peace of mind when it comes to preparing for our activities.
- Our plans should be living documents and correspond to our changing contexts.
- The tools and tactics we use should correspond to our threats.
- We constantly need to learn new tools and tactics as our context changes. This demands time and resources and, if possible, should be built into our strategic planning.

Appendix

Handout: Information Mapping

Information at rest

A simple way to start this cataloguing process is to think of the information as that which is primarily stationary (**at rest**) and that which travels (**in motion**).

Examples of this may be an old annual report document stored in a filing cabinet (information at rest), or having a phone conference planning meeting on an upcoming event (information in motion).

This distinction is used primarily as an arbitrary organising principle to help with the categorisation process. Where this organising principle can become useful is when we decide what tactics to employ in order to better secure our information, as there tend to be distinct ways of securing information at rest and information in motion.

Typically, information comes to rest in physical places like file cabinets, vaults, office desks, wallets, purses, shelves, books and ledgers. In the digital realm, we can think of file servers, computer drives, USB drives, SD cards, and CDs.

When brainstorming a list of your information at rest, it helps to also pay attention to some of its attributes, such as:

- Where are they?
- Who has access to them?
- How sensitive is their content to you, your organisation or people contained in the data (eg., witness or victim statements)?
- How important is it to keep them?
- How long should they be kept?

Typical threats to information 'at rest' in this sense might include:

- Data loss (through threats like virus infection, hardware deterioration).
- Unwanted access (through threats like confiscation, theft or spyware).

Ways we might protect our information 'at rest' include:

- Using free/open source software.[47]
- Practising good computer hygiene.[48]
- Having strong passwords, or a password management policy.[49]
- Encrypting files and hard drives.[50]

47 https://securityinabox.org/en/guide/malware
48 Ibid.
49 https://securityinabox.org/en/guide/passwords
50 https://securityinabox.org/en/guide/secure-file-storage

- Securely overwriting unwanted files.[51]
- Making regular backups.[52]

Creating an 'Information at Rest' map

Information Ecosystem

Considering all of the above, it is a useful exercise to create and maintain a map of your information (or your organisation's), by categorising your documents and the information related to your work.

This will help you understand the current state of your sensitive information, including who may have access to it, with a view to taking measures to protect it. This may include policies for who can access which data, as well as exploring technical options such as encryption. 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 as well, as the software itself can be thought of as a bundle of information.

Where does it reside? What are the physical places or entities where your information assets are kept? This includes 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? This is the *de facto* (actual) situation, not the aspirational situation. For example, in case of a person's folder of essays, the people who have access to it include the owner, any IT admin person who is in charge of the server, the person's confidant who knows where they are, etc.

How sensitive is it? There are many ways to classify the sensitivity of a document. The purpose here is for you to have a scale that is consistently applied to your information, which will help later on when you are assessing impact of incoming threats, etc.

A 3-tier scale is suggested here:

Secret: Only specific persons should have access to these. There is a clear chain of responsibility for this type of information (e.g. patient files in a clinic).

Confidential: These pieces of information are not for public consumption, but there is no specific need to preclude staff members of the organisation from access to these.

Public: These don't pose any risk of exposure to public. General policies still involve their integrity and safekeeping.

51 https://securityinabox.org/en/guide/destroy-sensitive-information
52 https://securityinabox.org/en/guide/backup

Map – Information at Rest

What	Attributes			
	Where does it reside?	Who can/ does access it?	How sensitive is it?	How should it be protected?
e.g. financial documents	*filing cabinet + hard drive*	*finance director, grant admin.*	*secret*	*locked cabinet, encrypted files*

Basic Text Cipher

Each letter corresponds to two numbers:

A = 11

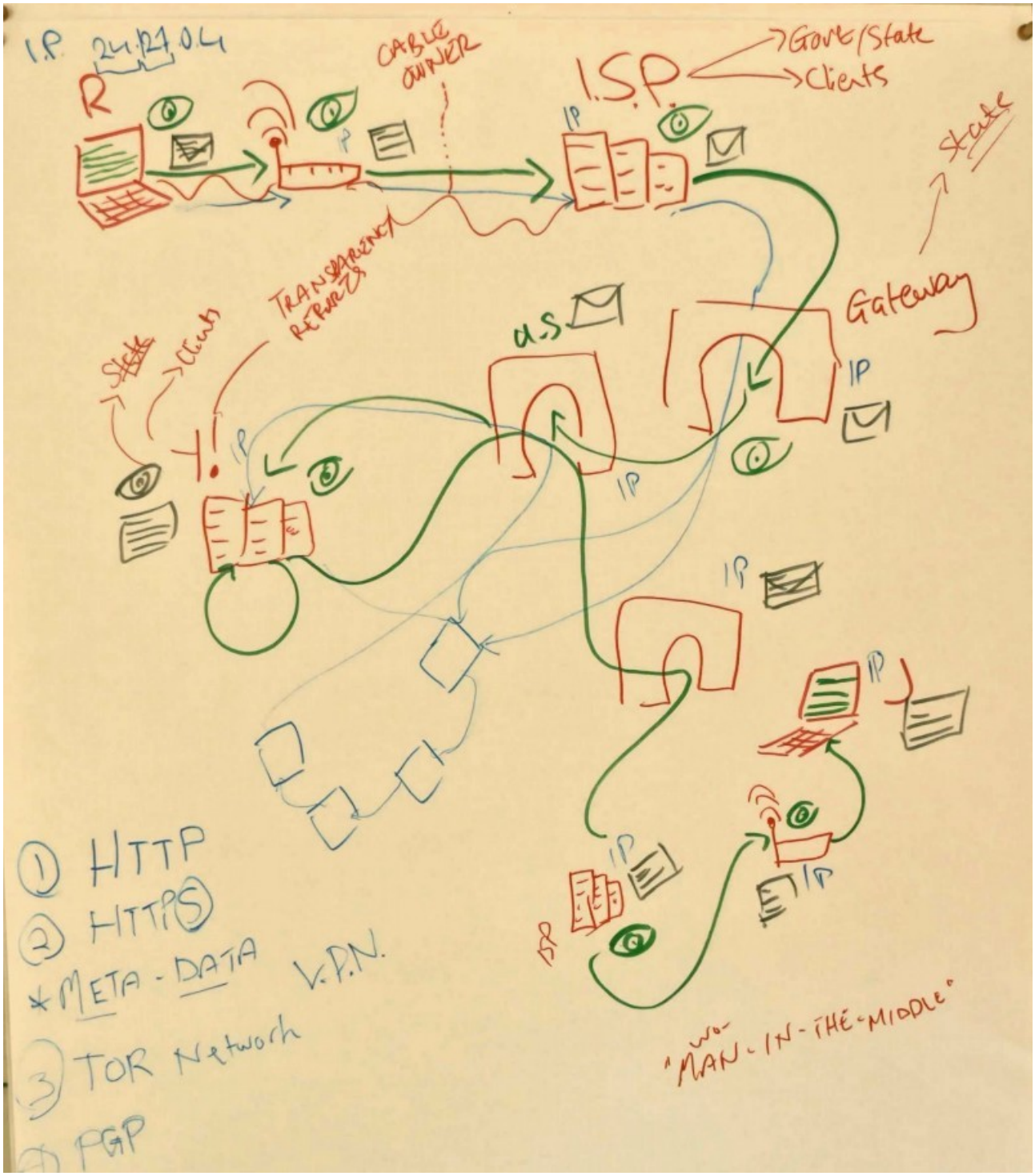
B = 12

N = 34

HELLO = 23 15 32 32 35

	1	**2**	**3**	**4**	**5**
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	W	X	Y
6	Z	!	?	,	.

Sample Flipchart Drawing – Information in Motion



Handout: Information in Motion[53]

Many of the information assets we have (especially in digital form) are at some point transported from one place to another. To be comprehensive, you might want to consider all possible ways your information may be in motion:

- the box full of documents you send to the archives via courier
- a phone call you make to have an important interview
- 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 forms of information (stored in physical devices) traversing physical space.

Note on digital forms of information:

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

Copy vs. original: Information in digital form is replicated constantly. During file transfers, email exchanges, uploads and downloads, and even when moved from one device to another, we are making copies of the information, which for all intents and purposes are identical to the original. This is slightly different from the pre-digital era where it was usually possible (though at times with effort) to distinguish between an original piece of information (e.g. minutes of a meeting typed on a sheet of paper) and its subsequent duplicate copies.

'Permanence' of information: Once a piece of information enters the internet, the process of upload, transfer and download includes multiple occasions where the information is copied. As our information travels across the internet, it may be retained somewhere 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, depending on the intentions of whoever controls the devices, for other purposes (e.g., surveillance, market research by companies).

It is therefore important to understand that a copy of a piece of information can be kept intentionally or unintentionally by one (or many) of these devices for a long time.

An example many people can relate to is an SMS 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 mobile network operator (MNO). The MNO 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. (Almost always, MNOs are required by law to keep copies of all SMS for a minimum length of time.)

Metadata: As computers and digital devices carry out their operations (creating and transferring information), a layer of 'metadata' is created. Metadata is information created about and by these

53 By Dan O'Cluanaigh, Ali Ravi and Peter Steudtner

processes themselves. Examples of metadata include:

- The location data of your mobile phone as it physically moves from one location to another.
- The senders, recipients and subjects of emails.
- Properties of an image file, such as the physical location where a picture was taken and the type of camera used.
- Properties of a document including information about the author, and the date in which a document was created or modified.

Metadata is often overlooked, because it is not something we ourselves create, or have explicit awareness about its scope or frequency. However, we can keep in mind its existence and take appropriate steps to understand possible ramifications when considering different elements in our information ecosystem.

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, including mobile phone calls, emails, VOIP (voice over IP), video chats, instant messaging, and SMS messages.
- Transfer data by uploading videos to the web, accessing a web page on our computer, backing up our documents to a server located somewhere else, or posting an update on Facebook.

Almost always, information travelling through digital channels is moving through physical space. For example, a status update starting on 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.

In order for us to contemplate the ways we can ensure its safety, it helps to consider the stations of information in motion:

- Where does it originate?
- What final destination does it arrive at?
- What path does it take on 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 our internet service provider(s), the telecoms companies which operate the internet infrastructure and transfer our data, and any entity that has control over these 'transit points' and may or may not be interested in capturing the data.

Therefore, 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 capture it along the way, or who would be interested in capturing it (consider your actor map)?

Protecting information in motion through digital channels

Some of the common ways we can protect our information as it moves through digital channels include:

- Using an SSL or HTTPS connection when we browse the internet.[54]
- Using a browser which facilitates anonymity, such as the Tor Browser.[55]
- Encrypting our emails with GPG/PGP.[56]
- Encrypting our chats with OTR (programs which facilitate this include Adium, Pidgin and Jitsi[57] [58]).

For more on the above, refer to **Security in-a-Box**.

54 https://securityinabox.org/en/guide/firefox/windows
55 https://securityinabox.org/en/guide/torbrowser/windows
56 https://securityinabox.org/en/guide/thunderbird/windows
57 https://securityinabox.org/en/guide/pidgin/windows
58 https://securityinabox.org/en/guide/jitsi/windows

Map – Information in Motion

What	Attributes				
	Method of transfer	Who has (or wants) access to it?	What physical or virtual routes does it take?	How sensitive is it?	How should it be protected?
e.g. emails among team members	*email (Gmail)*	*team members, email provider (Google)*	*Origin: staff computers* *Path: internet via Google servers* *Destination: staff computers*	*confidential*	*GPG encryption*

Handout: Practices for Identifying Digital Security Indicators

Scanning devices for malware or spyware

Especially for users of Windows and Mac OS computers, it's important to regularly scan your devices for malware and spyware. For more information on this, see the Avast![59] and Spybot[60] Hands-On Guides in Security in-a-Box.

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 manage which applications or programs can send and receive data over 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.

Check the task manager for any processes that look unfamiliar. 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 that 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 (or ‘two factor’) authentication,** which means that aside from knowing your password, you will need to input a code which 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 the computer. For example, you can do this by writing on parts with UV-marker which can't be detected without a UV light, or

59 https://securityinabox.org/en/guide/avast/windows
60 https://securityinabox.org/en/guide/spybot/windows

by using nail varnish with glitter, which will leave a pattern near impossible to replicate. Then check the markings regularly, especially after anyone else has, or may have had, access to your devices to see if everything is as it was.

Talking to your IT specialist

If you are working as an individual, it's good to maintain a relationship with a trusted IT specialist who can check your devices and ensure they are healthy. This doesn't necessarily have to be an expert, but perhaps even a friend who is more comfortable with computers.

Upgrade your knowledge 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 trustworthy and understand the kinds of risks and threats that human rights defenders can face to their information security. If you have such a person at your disposal, they can carry out regular checks on the organisation's devices and ensure their health, and should be able to answer your questions or take a look at your device if anything is amiss.

Sample register of security indicators

Date/ Time	Location	Reported By	Details	Discussion and Agreement