Appendices

Prepare
Explore
Strategise

Appendix A:

How Do I Use My Time?[1]

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

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

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

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

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

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

If yes, which meal? .....

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

If yes, which meals? .....

.....

.....

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

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

List those activities here: .....

.....

.....

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

Appendix B:

Scanning Digital Devices for Security Indicators

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

Scanning devices for malware or spyware

For users of Windows and Mac OS computers in particular, it's important to regularly scan your devices for malware and spyware. For more information on this, see the Avast! and Spybot tool guides in Security in-a-Box.[2,3]

Checking your firewall

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

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

Checking the task manager

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

Two-step authentication for accounts

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

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

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

Marking your devices and checking for tampering

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

Talking to a trusted and up to date IT specialist

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

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

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

---

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

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

Appendix C:

Analysing Declared Threats

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

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

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

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

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

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

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

Appendix D | Exercises 3.1c and 3.2a :

Identify New Capacities

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

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

Appendix E

Security Wheel[4] for Evaluating Organisational Security Management

Evaluation
Problems:
Solutions:

Aquired security experience
Problems:
Solutions:

Response to indicators and incidents
Problems:
Solutions:

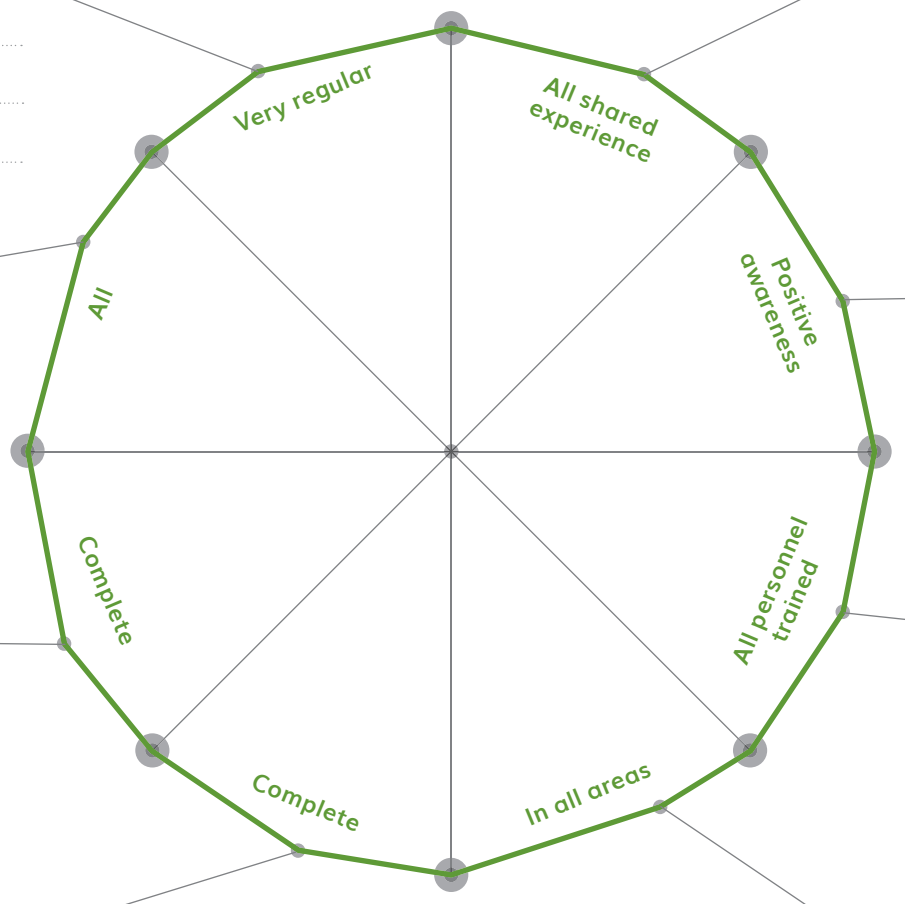
Attitude and awareness
Problems:
Solutions:

Ownership compliance
Problems:
Solutions:

Skills, knowledge, training
Problems:
Solutions:

Assignment of resonsibilites
Problems:
Solutions:

Security planning
Problems:
Solutions:



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

Appendix F

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

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

Appendix G

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

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

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