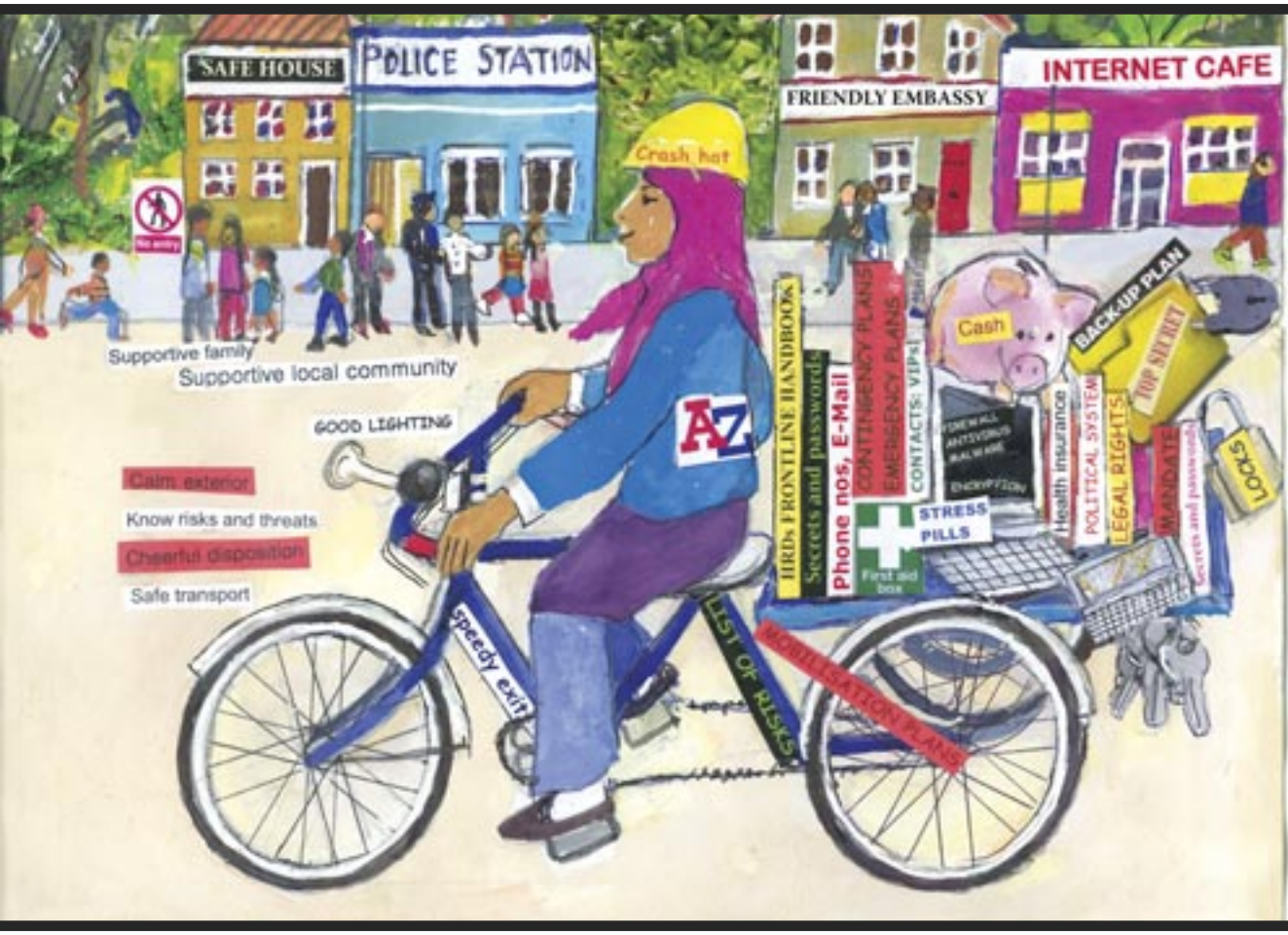
WORKBOOK ON SECURITY:

PRACTICAL STEPS FOR HUMAN RIGHTS DEFENDERS AT RISK



FRONT LINE DEFENDERS

APPENDIX 15

Surveillance Technology and Methodology

This check list is not intended to be a blueprint for security. Your own context is the key determining factor. Consider the risks and threats you face, and any vulnerabilities you have in order to supplement and personalise this list. See also the section on surveillance in Chapter 3, Analysing Threats.

Are you under surveillance?

- If you are not sure if you are under surveillance, assume you are and be very aware of what you say and do in order to protect yourself and others

- Discuss with other HRDs what surveillance methods are used in your country, what is the purpose (to collection information? to intimidate? to prepare for an abduction?) - your tactics will change depending on the objective of the perpetrators

- Discuss with your colleagues how you should react if you discover surveillance. For example if you find a tracking device on your car, should you leave it there or get rid of it?

A general rule seems to be – if you spot surveillance, pretend you haven't. If they see you are aware they will at best move further away and be harder to identify, and at worst become violent.

Dealing with surveillance technology and methodology

- **Microphones** can be microscopic and virtually undetectable by the human eye (eg in a jacket buttonhole – to tape your conversation), on a key fob (which someone puts down in on the table next to you), in a light fitting, wall or door of your meeting room, double-adapter plugs... but they need good sound quality
  - Don't hold sensitive conversations in your home, office or car. If this is not possible, choose noisy and/or unexpected places, eg laundry rooms (with the washing machine on), cleaner's closet...
  - If you are going to have somewhere swept for bugs, do not discuss it in that building, nor on the phone. Many microphones are sound-activated so do the sweep during a normal day under the guise of a normal activity such as having the room painted

- **Cameras** can be microscopic and hidden in TV screens, clocks, ornaments etc
  - Have good office and home security
  - Do not accept gifts from people you don't trust

- **Phones** can be tracked – both the sim card and the phone itself. Phone calls and text messages can be monitored. Phones could be loaded with a device or software and be used as microphones.
  - Do not leave your mobile phone unattended or lend it to people, even those you trust
  - Going to a sensitive meeting? Leave your phone at home. Or turn it off and take the battery out – ask all meeting participants to do the same
  - Skype to Skype conversations are believed to be relatively safe (but that could change...)
  - Public phone box to public phone box calls can also be relatively safe, but use different ones and never the ones nearest your home or office
  - Safest calls are from cheap unregistered Pay-as-you-go phones which are discarded after use

- **Vehicles** can have tracking devices installed on them
  - Get to know what your vehicle looks like underneath, check regularly, especially at the back of the vehicle (as the device has to communicate with a satellite)
  - Beware of who services your car, or recalls from the manufacturer to 'fix a problem'

Have a plan – if an HRD finds a device in their home or car, what should they do? Ignoring it whilst being aware of the implications and behaving accordingly could be the safest option.

Physical surveillance (being followed)

- Know that very professional surveillance operators may work completely unnoticed
- Practice situation awareness at all times (whilst resisting paranoia...):
  - describe people you see to yourself so you can recognise them again (consider who they remind you of, their height, walk - things that can't be disguised) Keep a notebook and write descriptions down as soon as practicable
  - who looks out of place? Are they wearing jackets/coats and/or carrying bags (to conceal surveillance equipment)?
  - notice vehicles - colour, make, and their occupants (perhaps they have maps, food and drink containers, are apparently talking to themselves etc)
- Don't be tempted to use the techniques you see in films (eg looking in shop windows for reflections, tying your shoelaces and looking around, speeding away from one car following you – these will be noticeable and ineffective). Instead act naturally at all times.
- All surveillance will have a 'start point' which will most likely be your home or work. Check
- Do not have a fixed routine. Vary the times and routes you use to go to work, go home, go to the gym, shopping etc.
- Align papers on your desk in a way so you know if it has been tampered with.

- **Vehicle surveillance:** a box system of 5 vehicles will probably be used – one ahead of you, 2 behind you and one to each side, perhaps on parallel roads
  - Don't bother speeding away – there is probably more than one vehicle
  - Drive naturally – don't keep moving your head to look in your rear mirrors
  - To check for surveillance, turn into a cul-de-sac or a petrol station to get fuel – but be careful that it looks natural
  - To evade surveillance park somewhere and then, in a relaxed way, jump onto public transport

- **Attending sensitive meetings:** Arrange a simple code for sensitive meetings, eg "I'll meet you on Tuesday at 11 am" means "I'll meet you on Monday at 10 am" (a day and an hour earlier)
  - Safest meeting places are noisy, popular cafés where the seats are not allocated (and microphones will be impossible to install where you are going to sit
  - When you meet face-to-face at a safe place, use the opportunity to agree codes for the future or give an encryption key

If you see an increase in physical surveillance (cars, operatives etc) and it becomes more open, it could be an indication that you are going to be detained. Do not follow your regular pattern as soon as you notice this. Consider relocation to a safe house.

Finally:

Many people innocently reveal information about themselves and their whereabouts, through:

- business cards (have one with your mobile phone number and safe email address which is only given to trusted friends)
- Facebook or other social networking sites – your profile can reveal your vulnerabilities and reveal where you are, who you are with...