

PART III

PROTOCOLS, EMERGENCY PLANS AND MORE POLICIES

In the third part of this Manual, we are putting forward the logic for drawing up protocols, emergency plans (for use in specific situations), and more security policies.

They are based on good practices shared and learnt in the workshops we run.

They are however neither complete nor a guarantee of good results, as the manual cannot reproduce all the variables of a given context.

This is very much a work in progress, on which we welcome your feedback, as well as new suggestions for protocols and plans.

We will publish updates and developments on the website www.protectionline.org, so that defenders can benefit from them as soon as possible, and we will include all developments in our next edition of the manual. Meanwhile, please refer to Annex IV - *General Risk Outline for Specific Human Rights Defender Profile*.

CONTENTS OF THIRD PART:

- 3.1** How to reduce the risks connected to an office search
- 3.2** Detention, arrest, abduction or kidnapping of a defender
- 3.3** Secure management of information
- 3.4** Security and free time

How to reduce the risks connected to an office search and/or a break in

A search may best be described as the forced entry into a house, office, or a private space. A search is legal when it is the State that decides about it and carries it out according to laws in force. A search is illegal when the forced entry is against the law (for example a robbery during the night, a search by security forces without the necessary search warrant or a forced search by an armed actor.)

Although the case that follows is the result of a legal search, defenders will also be able to extract rules applicable to illegal searches and complete them with information contained in the chapter on security of houses and offices.

The State may lawfully carry out a search. The law in force will need to be in line with the international standards on human rights and the protection of democratic freedoms. However, it can be a serious problem if, against international standard, searches are used as a standard method to continually harass and pursue in justice human rights defenders and social movements through routine searches.

No defender can claim that a search is an “unexpected” event (as with any other risks), all the more that a search can be absolutely legal. No risk can be reduced to zero. We then need to reduce as much as possible the related threats/ consequences of the search risk.

How do we achieve this? By using the risk equation and listing all threats/consequences (consequences may be assimilated to threats). Then, for each threat/consequence, list the related vulnerabilities and capacities, and start working on them...

Threats/consequences linked to searches.

A search generates threats/consequences:

- a • The threat that during a search somebody may suffer physical or psychological harm.
- b • The threat that information may be taken away, lost or destroyed.

- c • Related to that, that information may then be used inappropriately by a third party.
- d • The threat that contentious objects may be “hidden” (arms, drugs, documents) in order later to proceed “legally” against the organisation.
- e • The threat/consequence of money and specific properties (such as computers,...) being stolen or destroyed.
- f • ...

a ♦ The threat that during a search somebody may suffer physical or psychological harm.

No one can predict how a search will be carried out and what its impact will be. However, having as much advance information as possible about a search can contribute to avoiding behaviour and stress that could add to the likelihood of physical and psychological harm. It can contribute to raising awareness of risk triggers and to maintaining positive behaviour.

Vulnerabilities:

- not knowing what a search is about
- believing that opposing it will help the situation
- no medical insurance
- ...

Capacities:

- knowing how a legal search may be carried out
- knowing what department may issue search warrants and being in possession of the name of the current responsible officer (before and during a legal search)
- knowing what a search warrant looks like
- knowing what the legal rights of the searched organisation/individual are (including the right to ask to see the search warrant and possibly to request legal assistance)
- having access to legal assistance (during and after the search)
- how not to put up undue resistance
- if a search is carried out with violence, it is important that the people stay in a group to reduce the risk of being mistreated individually
- ...

The organisation consider posting in a visible place:

- a sample search warrant

- all corresponding legislation (rights and duties of both parties)
- a list with the names and telephone of the organisation's lawyer, doctor, psychologist, the closest hospital...(This list should also be visible in other parts of the office so as to increase the possibility of quick access to it by staff members present)

This information is legal and public. It can therefore be visually accessible by both parties. This may not prevent a search (either with or without a search warrant). It might however help to reduce stress among those being searched. It might also contribute to notifying the searcher that the searched individual or organisation is aware of their rights and that they will take action later in case the search goes beyond legal prescript (deterrence).

b ♦ The threat that information may be taken away, lost or destroyed.

In general, most organisations keep more information than is needed. Of this, a high amount is hardly ever used and is not confidential. In other words, only a small amount is confidential and this should not be accessible to searchers. Absolutely confidential information usually includes: lists of people (project beneficiaries, witnesses in cases); crucial evidence in legal cases; specific cases and analysis.

Information deemed public or not contentious can be kept in the office for the searchers to take (such as one does when travelling with money, keeping visible only the amount we can afford to lose to robbers).

A proper information security policy means that many of the consequences connected to the loss, theft or destruction of information are considerably reduced.

It also means that the defender should not feel the need to expose themselves to protect information (in any case, life must come first) ; this will decrease the likely stress generated by the search, thus reducing the risk of violence and injuries both physical and psychological (taking care of the above threat/consequences).

Vulnerabilities:

- information not stored/filed according to agreed distinction between confidential or not.
- sensitive information held on paper
- electronic information not encrypted (files and attachments).
- inadequate office and house security: not enough barriers and filters to prevent access by undesirables or at least allow time to shut down a computer or hide a document.
- ...

Capacities:

- regular backup copies (at least weekly) of information stored on computers, and kept in a safe place. In case of a search you will therefore largely know how much information is actually exposed (depending on the date of the search vs. date of the last back up / storage of information)
- copies or photocopies, or even better, scanned copies, for keeping records of essential documents in a safe place. If necessary they can be distributed around other safe places).
- adequate office and house security measures.
- warning at the beginning of a search in order to obtain legal support (lawyers) and requests from other organisations to provide assistance and witness the search, at least from outside. This will put pressure on the perpetrators in the hope that they will comply with the law during searches.
- ...

COMPARISON OF DIFFERENT COMPUTER BACKUP SYSTEMS

Storage medium	Advantages	Disadvantages
CDs/DVDs burning	Many computers have CD/DVDs burners. Easy and safer transportation and storage of the backup DVDs/CDs.	In case of a high amount of information, many CDs are needed, which makes the whole process longer and more complex. Anyone managing to obtain the CDs will have access to all the data.
Flash disk	Same as above.	As above though easier to store and therefore, less likely to fall on unwanted hands.
External hardware	Holds a lot of information and it doesn't take much time to copy over. Can be equipped with access codes in order to protect the information.	Cost (200-300 US \$).
Server at a remote location	Can hold all the information, is quick, cannot get lost or stolen.	You need a broad band internet connection and encryption Server companies might be 'forced' to give the archive to the searchers ('state security claim').

c ♦ The threat/consequence of the information being taken away and used by the third party.

High likelihood of consequences for the organisation and for the people mentioned by the information.

Consequences for the searched organisation

Vulnerabilities:

- no advance consideration given to possible reaction procedures
- neglecting ethics, bad accounting, pirated software (might mean legal proceedings against the organisation)
- ...

Capacities:

- Back up copies
- Reaction plan in place
- ...

Consequences for the people mentioned on the information.

Vulnerabilities:

- not having previously discussed the possibility with the people involved
- not having fast access to them
- ...

Capacities:

- to have explained the existence of the risk and made as sure as possible that it will not happen out of the negligence of organisation/people.
- to have planned together the emergency reaction (resorting rapidly to the plan, , protection measures, hiding places, etc)
- ...

d ♦ The threat that contentious objects may be “hidden” (arms, drugs, documents) in order later to proceed “legally” against the organisation

Vulnerabilities:

- office space is full of objects and papers not related to work (personal objects, scattered magazines... (it is more difficult to spot if something is being hidden intentionally during the search, or if a previous visitor has hidden/left a contentious object/document which might then be “casually” found by the searchers

- no inventory of office material at all, let alone a recommended registered inventory with a lawyer
- only one organisation person present during the search
- ...

Capacities:

- where possible, (in the case of a legal search)¹, people are prepared to arrange themselves in the various corners/rooms of the office (for example each person on his/her working place) so as to be able to observe what happens during the search. it is also easier this way to notice if anything is being taken illegally.
- after the search (no matter what type of search), the organisation carries out a complete check of the office or place (if possible with the assistance of external observers), recording (even photos) all that can be found and making sure that what does not belong to the office/was not there before the search, is clearly reported and not touched (be aware of finger prints). Make a record also of missing items.
- File a report with the police and follow legal provisions in force.
- ...

e ♦ The threat/consequence of money and specific properties (like computers,...) being stolen or destroyed.

An illegal search will most probably will entail the theft of items.

Vulnerabilities:

- high amount of money and valuables kept in the office
- unprotected items
- no inventory of office material at all, let alone the recommended registered inventory with a lawyer
- no insurance against theft
- ...

Capacities:

- arrange office staff in various places in the office in order to observe the search²

¹If a search is carried out with violence, it is important that the people stay in a group to reduce the risk of being mistreated individually

²Again, if a search is carried out with violence, it is important that the people stay in a group to reduce the risk of being mistreated individually

- warning at the start of a search in order to obtain legal support (lawyers) and so that other organisations may be requested to provide assistance and observe the search, at least from outside. This will put pressure on the perpetrators in the hope that they will comply with the law during searches
- ...

How to confront and reduce the threat of the search itself.

If a search follows the standard international legislation and has a legal and legitimate goal then there is no point in even thinking about confronting or reducing the threat of a search. You have to open the door and consider only the previous steps on acting on the consequences. However, if searches are used as a systematic way to hinder the work of HRD and social organisations, then corresponding action should be taken.

In order to confront and reduce the threat of a legal search, the best strategy is to raise their political cost through public campaigns and advocacy, preferably in collaboration with other organisations and institutions.

If there is a risk of an illegal search (or robbery) it is important to improve as much as possible the security of the house, office or the premises.

This all applies whether your office/home is in an urban or a rural area.

Summary

How to reduce the risk of a search.

Searches can be both legal and illegal (when illegal it is akin to breaking in).

And just as for any other specific risk, increase the political cost of searches

Use the equation and unfold each element as far as you can go.

List the threats/consequences and their respective vulnerabilities and capacities and work on them:

- a** ● The threat that during a search somebody may suffer physical or psychological harm.
- b** ● The threat that information may be taken away, lost or destroyed.
- c** ● Related to that, that information may then be used inadequately by the third party.
- d** ● The threat that contentious objects may be "hidden" (arms, drugs, documents) in order later to proceed "legally" against the organisation
- e** ● The threat/consequence of money and specific properties (such as computers,...) being stolen or destroyed.
- f** ● ...