4

Understanding and Cataloguing our Information

This Chapter involves understanding what 'information' actually means in relation to our activities and goals as activists. The importance of information management cannot be underestimated, especially given the growing use of digital technologies in the context of defending and promoting human rights. While these tools offer us great potential for communicating, researching, organising, and campaigning, they are also a key target for our adversaries seeking to place us under surveillance, gather information or hinder our work.

When we talk about 'information' in the context of our work, we refer to many things, such as:

- The outcome of the work we are doing; such as a report, a database of human rights violations, images, voice and video recordings.
- Operational information that helps us do our work; such as our text messages during an action, our files and progress reports and other office information and communication, including financial, human resources and strategic organisational documents.
- Personal information that identifies who we are both as members of an organisation, as well as other personal or professional affiliations.
- Data generated by our use of digital devices as we work, or 'meta-data', which can be used to track our movements or monitor our relationships.

This information can be stored and communicated in many ways: on paper, on our computers, on mobile phones, on the internet, on file servers, various internet services and social networking outlets. Taken together, this information comprises one of the most important assets any of us (or any organisation) has. As with any asset, we are best served when we are sure that this asset is properly cared for so it doesn't accidentally or maliciously get lost, corrupted, compromised, stolen or misused.

In caring for our own security, we need to care for the security of our information. Information about us, our activities and our plans can be very useful to our opponents and with the increasing use of digital devices and social media, it is imperative that we make sure we remain in charge of who has and controls our information. Surveillance and information gathering have always been used to plan attacks against human rights defenders, and such invasion of the right to privacy could itself be considered a form of (often gender-based) violence.

Common threats to HRDs' information

Data loss

Due to poor computer hygiene, malware infections, power cuts or ageing hardware, computers and other devices occasionally cease to function causing us to lose our data.

Compromised accounts

Sometimes, our passwords or 'secret questions' are not very difficult to break, or we are subjected to phishing attacks (which can be random or targeted for us especially) and unknowingly hand them over to a third party, who gains access to our email or social media accounts.

Device confiscation or theft

Computers and mobile phones are common targets for thieves. Furthermore, if we face acute risk, our offices and homes may be raided by State or non-State actors and computers, mobile phones, hard drives, USB keys and servers could be 'confiscated' or stolen for analysis.

Device inspection at checkpoints

Sometimes we may have our devices temporarily confiscated while crossing borders or military checkpoints, where the data may be copied or the computer may be infected with spyware or have a hardware keylogger attached.

Information handover

Internet service providers and the providers of the email and social networking sites that we use can also hand over our data to certain authorities if a legal request is made to do so. While they protect our data from some, they are more willing to hand it over to others, and this situation is constantly changing in accordance with business and political interests.

Surveillance and monitoring

Data brokers, internet service providers, email providers and many other companies subject the general population to surveillance by gathering and aggregating details of our online activities. While in some cases this has the aim of merely targeting us with advertisements, it can also be used to identify particular minorities to which we may belong as a target for deeper surveillance.

Targeted malware

Targeted malware is a growing industry: some State authorities and other groups invest in software which is designed to trick us into downloading it and later granting the attacker access to much or all of the data on our devices.

The security of our information is critically important and so protecting it can become a source of anxiety. An effective and up-to-date information security strategy can give us the peace of mind needed to focus on our objectives and carry out our work in a healthy way.

The first step involves a process of cataloguing, as much as possible, all instances or versions of our information. Creating a mental understanding of what elements exist in our own information ‘ecosystem’ will help us move away from perceiving ‘information’ as a vague mass of data, towards a better understanding of it as a tangible and important asset.

By cataloguing our information into various components and types, we can identify any potential situations and avenues where our information may be or may become vulnerable, as well as areas where we need to improve its safekeeping.

This process relies on the output of the previous exercises where we identified the ‘actors’ in our context, including ourselves, our allies opponents and currently neutral parties. We may refer back and expand the actor map with potential new actors identified through the information mapping process. The map will also facilitate understanding of the relationship between elements of our information and our allies and opponents and their intentions and abilities.

Next we look at some key concepts for understanding how to catalogue our information, followed by the ‘information ecosystem’ exercise which will help us generate a map of our most important information assets.

Categories of information

The first step to creating an information security strategy is to get to know what information we have, where it is, and how it moves from one place to another.

A simple way to start this cataloguing process is to think of the information in terms of what is primarily stationary (at rest) and information which travels (in motion). Examples of this may be financial information stored in a filing cabinet (information at rest) versus exchanging messages via mobile phone on an upcoming event (information in motion).

This distinction is used primarily as an organising principle to help with the categorisation process. It is important to remember that today much of our information is in digital form, and with increasing use of the internet and remote storage services (i.e. 'the Cloud'), much of the information we possess is at one time or another in motion. Similarly, due to the growing popularity of hand-held devices (such as smartphones and tablets), increasing storage capacity and the actual mobility of these devices, any information stored on such devices, although it may be digitally 'at rest', is actually moving in physical space.

It is worth repeating that under the above categorisation, our communications – such as emails, chats, text messages and phone calls are 'information in motion', and that this is extremely common, especially in the context of having near constant connectivity over the internet. Where this organising principle can become useful is when we decide what tactics to employ in order to better secure our information, as there are distinct ways of securing information at rest and information in motion.

Information at rest

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

It is important to explicitly list them and consider, in the first instance, whether or not they are appropriate for achieving the objective we have set. Our work does not take place in a vacuum, but rather in a rich and diverse context, often with some characteristics of conflict. Our activities are our 'interface' with this conflict and with the State and the society that we are trying to influence; they are our means of attempting to change the situations, the perceptions and behaviours of a diverse set of actors (individuals, institutions and organisations) around us. Some of these actors will benefit from, believe in and support our activities. Others, however, will feel that these activities are not in their interest and will attempt to close our space for work.

All of these can often provide a source of information about a person, a project, a movement or an organisation and for this reason, theft and confiscation of computers, phones, and memory storage devices are common tactics of human rights defenders' opponents.

When brainstorming a list of your 'information at rest', it helps to consider some attributes, such as:

- where they are
- who has access to them
- how sensitive is their content to you, your organisation or people mentioned in the document (e.g. witness or victim statements)
- how important it is to keep them
- how long they should be kept.

Information in motion

As mentioned before, many of the information assets we have (especially in digital form) are at some point transported from one place to another. Consider all the ways your information may be moving:

- the box full of documents you send to the archives via courier
- a phone call you make over the mobile network
- videos of an event you upload to a server online
- the contact information in your mobile phone as you participate in a protest.

In the examples above, we can see various ways our information is in motion: physical pieces of information travelling in physical space, or digital information travelling through the internet, or digital information (stored in physical devices) traversing physical space.

We should also pay attention to the different ways information can travel:

- **Transfer:** Whether during an office move, or when an attachment is sent to a colleague over the internet, or a backup of sensitive files is made to a server in another location, our information is transferred from one point to another.

- **Communications:** When we interact with our colleagues, allies, the public and indeed opponents, there is an exchange of information that takes place. Communication can take the form of announcing instructions from a loudspeaker at an event, or exchanging confidential information during a phone conversation, a video-call, an in-person meeting, emails, text messages and many others. Our communication contains lots of information about our intentions, the status of our action, and our plans and future activities.

To catalogue such information, in addition to the attributes mentioned for 'information at rest', you can also think about:

- how the information is transferred
- what physical or virtual routes it takes
- who may be able to access it along the way, or who would be interested in capturing it (consider your actor map)?

Digital forms of information

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

- **Replication:** Information in digital form is constantly replicated. During file transfers, email exchanges, uploads and downloads, and even when moved from one device to another, copies of the information are created, which for all intents and purposes are identical to the original. This is slightly different from the pre-digital era where it was possible (though at times difficult) to distinguish between an original piece of information (e.g. minutes of a meeting typed on a sheet of paper) and subsequent duplicate copies.
- **'Permanence' of information:** As noted above, once a piece of information is uploaded to the internet, the process of upload, transfer and download entails multiple occasions where the information is copied. It follows that our information may be retained somewhere as it is traversing parts of internet which we don't control (as often is the case). Copying and relaying happens as mail-servers, routers and intermediary locations make copies of the information to aid the transfer process, or for other purposes, depending on the intentions of whoever controls the devices. It is therefore important to understand that it is possible for a copy of a piece of information to be kept intentionally or unintentionally by one (or many) of these actors for a long time.

An example many people can relate to is a text message. These messages are sent from one mobile phone to another, but as they are sent, they pass through a number of cell towers and other infrastructure which belongs to the service provider. The service provider has access to these messages and will, in most cases, retain them for a period of time, regardless of whether you delete them from your telephone or not.

- **Metadata:** As computers and digital devices carry out their operations, a layer of 'metadata' is created. Metadata is information created about and by these processes themselves. This information accompanies the data itself, and sometimes it cannot be removed from the data. Examples of metadata include:
  - Your **IP address** which locates where you are connecting to the internet, and the IP addresses of the websites you visit.
  - the **location data** of your mobile phone as it moves from one point to another, **the unique identifying numbers of the SIM card and of the phone** (known as the IMEI number). It is generally not possible to change your phone's IMEI.
  - **the senders, recipients, time-stamps and subjects of emails, and whether they include attachments**. This information cannot be erased, as servers need to know who to send the emails and its attachments. However, some of it can be changed or obscured.
  - **properties of an image file**, i.e. information about the location in which a picture was taken, its size and the equipment used to produce the image (brand of camera and lens, software used to edit it) Some of this information can be erased using image processing software.
  - **properties of a document**, i.e. information about the author, the date in which a document was created or modified. Some of this information can be erased by changing the personal privacy settings of word or spreadsheets processors, or using a metadata stripping software such as the Metadata Anonymization Toolkit.[10]

Metadata is often overlooked because it is not something we ourselves create or may even be aware of. However, we should keep in mind its existence and take appropriate steps to understand its scope and the possible ramifications when considering different elements of our information ecosystem.

[10] See https://mat.boum.org

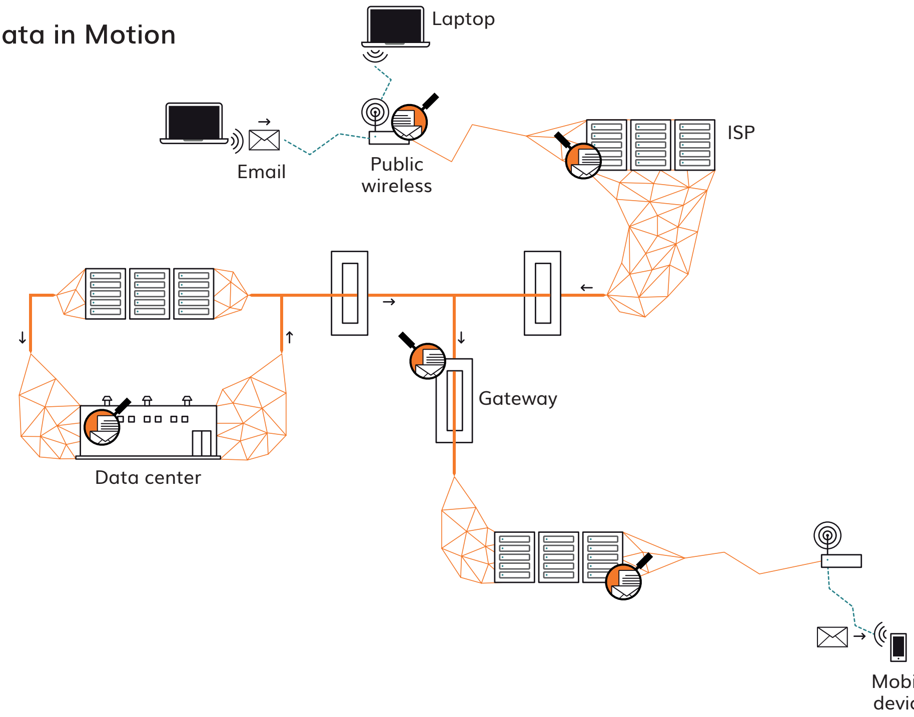
Understanding information in motion through digital channels

The above attributes of digital forms of information play an important role when we think of our information in motion through digital channels, since information can be so readily duplicated and stored. Information is in motion through digital channels when we:

- communicate using our devices; call via mobile phone, send emails, make calls using voice-over-IP, video chats, instant messaging or send text messages.
- transfer data; upload videos to the web, access a web page on our computer, back up our documents to a server located somewhere else, post an update on social media.

Information travelling through digital channels is almost always moving through physical space, e.g. a status update starting at your mobile phone will make its way to the social media website, which is physically stored on servers in a particular location, perhaps on the other side of the world. It may pass through a number of different countries along the way. In order for us to contemplate the ways we can ensure the safety of our information in motion, it helps to consider its origin, destination and the path it takes along the way.

Data in Motion



While we may know where our information originates (e.g. we type an email on our laptop), we need to pay attention to where it will end up (e.g. our colleague's inbox via their mail provider), as well as all the stops along the way, including:

- internet service provider(s)
- the telecom companies which operate internet infrastructure and transfer our data
- State entities who carry out active capturing and surveillance of data and metadata as it is transferred through the internet
- any other entity that has control over these stops and may or may not be interested in capturing the data
- other third parties like advertising companies who may gather data about our online activities.

The process of information moving digitally between spaces is relatively straightforward. Taking the time to learn or review the basics of how internet and mobile communication work helps us clarify this process. Doing so can reduce our anxiety or unfounded fears which may arise from misinformation, myths and mysteries associated with digital technology and electronic surveillance.

Consider also including the type of encryption (if any) that is used to protect the data. Encryption is a technical means of reducing the number of people who can access certain information. It is ocasionally provided by service providers (for example, banking websites or certain communication applications[11]), although often we must learn to encrypt our information or communications using particular software in order to be more certain that it won't be accessed.

Contemplating the above is also important as it may suggest additions to our actor map. We may discover we need to investigate whether there is any relationship between these actors and our allies or opponents. Having reflected on this, you may want to return to your actor map and include actors such as:

- your internet or website service provider(s)
- your telephone service providers
- providers of your email and social networking services
- any relevant entities (e.g. government agencies) who may have a relationship to the above.

These additions create a clearer picture of what exists in our information ecosystem, as well as listing any additional actors who may be involved in our work as a consequence of how our information is handled. This knowledge will equip us

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

to protect our information more effectively. This may be through implementing policies about who can access which information, or using software which protects our information, such as for securely deleting data from our devices or encrypting our chats and emails.

In the next segment we will undertake an exercise to map our information 'at rest' and our information 'in motion'. This will help us identify the gaps in our information management practices as well as ways of bridging those gaps.

Mapping your information ecosystem

Considering all of the above, it is a useful exercise to create and maintain a map of your information, or that of your organisation, which categorises your documents and the information related to your work. This will help you to understand the current state of your sensitive information and who may have access to it, with a view to taking measures to protect it. This may include policies for who can access what data, as well as technical methods such as encryption.

This 'information map' can take the form of a text document or spreadsheet which can be regularly updated. In the following exercise, we will walk through the steps involved in creating such a document, and provide an example template which could be useful.

When creating an information map, it is useful to consider the following questions:

What information is it?

An organising principle here is to group similar types of information together. For instance, you can decide that all financial documents belong in the same category, whereas not all emails belong together. Grouping the 'what' according to type of information largely depends on the way you and your organisation work. Include software that you use here too, as the software itself can be thought of as a bundle of information, and some software can be considered sensitive.

As mentioned previously, one type of information we often don't consider with regard to digital files and communications, is meta-data. Especially with regard to information 'in motion', it is a good idea to include the meta-data of certain documents and communications (such as pictures and email files) and consider whether it needs to be removed or distorted to protect your privacy.[12]

[12] For more on how to remove metadata from files, see https://securityinabox.org/en/lgbti-mena/remove-metadata and for how to remain anonymous online see https://securityinabox.org/en/guide/anonymity-and-circumvention

Where does it reside? What are the physical places or entities where your information assets are kept? These may include: file servers in the office, web servers at service providers, email servers, laptops/computers, external hard-drives, USB drives, SD cards and mobile phones.

Who has access to it? Consider the situation here as it currently is, rather than the aspirational situation. For example, in case of a person's folder of reports on an office computer, the people who have access to it may include: the person themselves, any IT admin staff in charge of the server, the person's confidant, etc.

How sensitive is it? There are many ways to classify the sensitivity of a document. It is a good idea to establish an explicit categorisation for sensitive information with clear instructions on how it is to be protected. The purpose here is for you to have a scale that is consistently applied to your information which will help identify the data which is most likely to be under threat and the means by which it should be protected.

Below is an example of a three-tiered scale:

- **Secret:** only specific persons should have access to this information. There is a clear chain of responsibility for this type of information (e.g. patient files in a clinic).
- **Confidential:** this type of information is not for public consumption, but there is no specific need to preclude staff members of the organisation from access to these.
- **Public:** this type of information does not pose any risk of exposure to public. General policies however still involve their integrity and safekeeping.

It's worth noting that, in the life-cycle of a project, the sensitivity of the data involved may change. For example, if we are investigating torture in order to later make a public report about it, many of the details involved will initially be secret or confidential. Later in the project, once the data is gathered, that which must remain confidential will be separated from that which must be made public as part of the report.

Considering our information in light of these questions, we can create a document which represents a map of our information as it currently is. However, as noted above, it's important to remember that this is a live document and should be regularly updated.

2.4 Exercise

Information ecosystem

Purpose & Output

The purpose of this exercise is to take an inventory of the most important information assets you manage, in order to create policies for its safekeeping later on.

Input & Materials

It may be helpful to reproduce the example table below, either by printing it or drawing it on a flip-chart or other materials.

Format & Steps

Brainstorming and documentation

To begin the exercise – especially in a group – it may be useful to use a spreadsheet, or a large sheet and sticky notes, or some other means which allow you to brainstorm easily and group things together.

Brainstorm and make a list of all of the data you manage. If you're not sure where to begin, consider:

- data related to each of your human rights activities
- personal data and files, especially if stored on your work computer
- browsing activities online, especially of sensitive data
- emails, text messages and other communication related to your human rights activities.

Imagine a spreadsheet that has several columns enumerating categories as described below. Your task is to fill the rows with information.

Start with your information at rest, and for each type of information, elaborate on the following

- what information is it?
- where does it reside?
- who has access to it?

Format & Steps

- how sensitive is it?
  - secret
  - confidential
  - public
- how important is it to keep it?
- who has access to it?
- how should it be protected?
- how long should it be kept before destroyed?

Characterise and qualify the information you have mapped out. You can repeat the same process and expand the spreadsheet with additional entries for your information in motion; e.g. data being transferred (physically, electronically), communications over the internet or telecommunications networks.

The questions and example in Table 2 below may help you with this.

Remarks & Tips

This process is iterative. Once you have done the first round, you may detect patterns and groupings. For instance, you may decide that since all financial information (regardless of type) has similar sensitivities and longevity, you can group them and think of them as a financial information category.

Conversely, you might find yourself needing to expand a row into several rows. For instance, a row containing ‘email’ needs to be expanded to several rows to account for a subset of emails – and their safe-keeping – which is sensitive.

This should be a live document and will change according to shifts and developments in your situation. So you will benefit from regularly updating this document to account for any of these changes.

Table 1.

Information at rest				
What (examples)	**Attributes**			
	Where does it reside?	**Who can/does access it?**	**How sensitive is it?**	**How should it be protected?**
Financial documents in electronic form	Secure shared folder – file server	Executive team	Secret	Saved in hidden encrypted partition. Backed up daily to encrypted hard-drive
Program reports for the censorship campaign	Documents folder – file server	Team members, program director	Confidential	Saved in encrypted partition
Adobe InDesign for the web developer	Web content manager's laptop	Web content manager	Confidential	Licensed, password-protected

Table 2.

Information in motion					
What (examples)	**Attributes**				
	What method of transfer are you using?	Who has (or wants) access to it?	What physical or virtual routes does it take (origin, path, destination)?	How sensitive is it?	How should it be protected?
General emails among team members	Email (Gmail)	Team members, email provider	**Origin:** staff computers **Path:** internet (via Google servers **Destination:** staff computers	Confidential	GPG encryption
Check-ins during missions	Text messages (SMS)	Team members, telecom company	**Origin:** mobile phone **Path:** mobile network **Destination:** mobile phone	Secret	Code words

At this point you will have your initial document describing your/your organisation's information ecosystem, which, along with the map of actors, will be invaluable as you begin the process of understanding your strength and resilience, as well as areas where you may be weak or vulnerable.

You can then begin to chart a path from identified security indicators, to specific threat scenarios, to designing strategies, plans, tools and tactics which can help you avoid these types of scenarios, or minimise their effect.

By now, we have:

- mapped out who our allies and opponents are, and the neutral parties who may become allies or opponents depending on the situation
- listed some of the relationships we, our allies, and opponents have
- created our own information ecosystem document which helps us understand and prioritise our information as it rests somewhere, or while it is travelling through various channels.

In the next Chapter we will shift our analysis to the indicators we encounter in the course of our work which may alert us to potential threats and how to systematise our knowledge of them in order to take action.