Earth Defenders Toolkit

Guide: Personal and physical safety for earth defenders

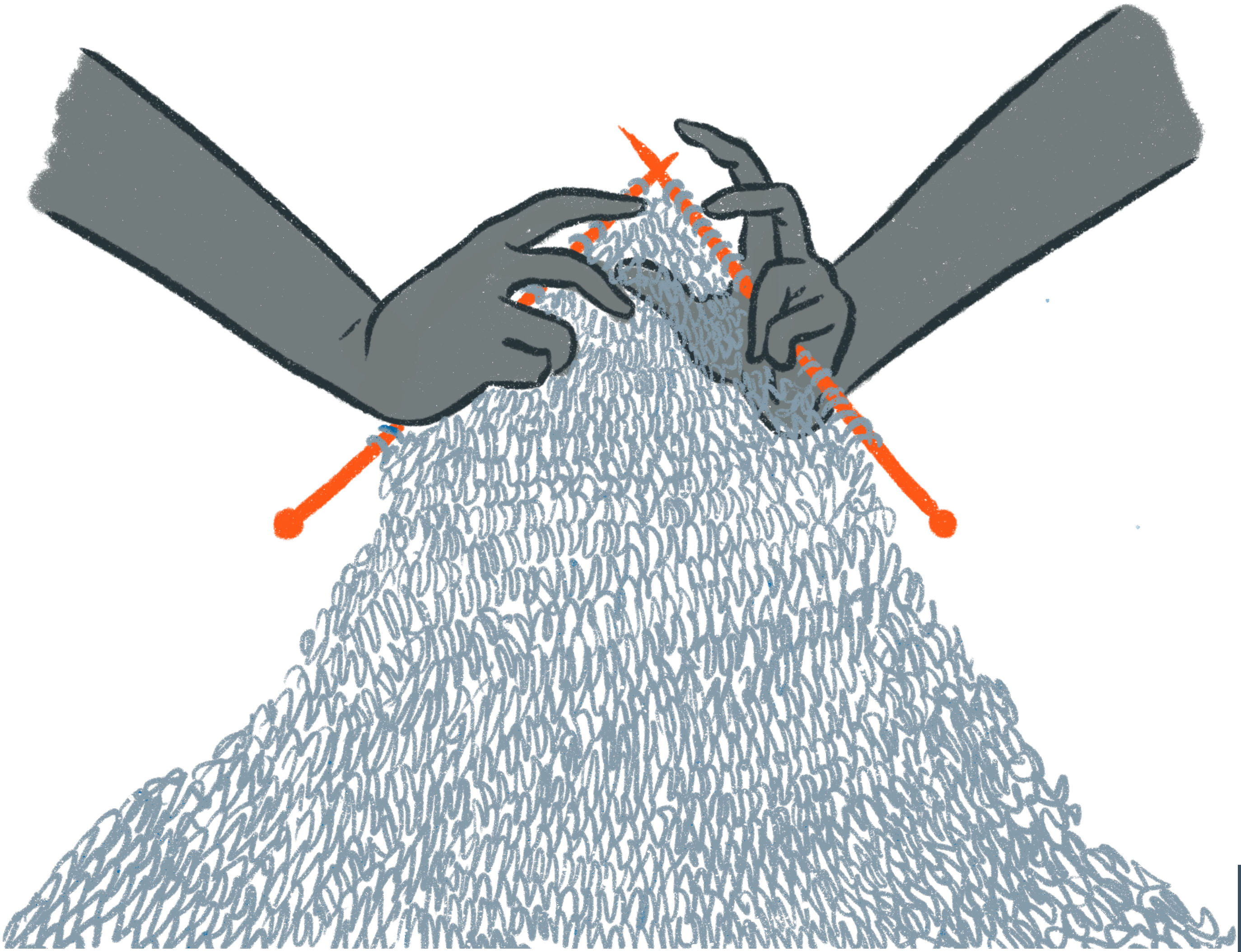
Why be concerned about personal safety?

Being an earth defender is neither easy nor safe work. On many occasions, earth defenders are criminalized, threatened, imprisoned, and attacked by actors whose interests conflict with theirs. **Hundreds of defenders are murdered every year** worldwide, and in some regions, the attacks are increasing at an alarming rate. The aggressors range from small illegal resource extractors to **big corporations, private security firms, and even government agents.**

Due to these concerns, security considerations - ranging from digital security to personal safety - are a key aspect for most environmental and human rights-based projects. This work usually involves collecting sensitive data and often takes place in areas of conflict over land or resources. As such, both the collected data and the teams involved face threats from anyone aiming to jeopardize the work or gain access to the data or knowledge.

Due to the range and diversity of project contexts, we cannot provide a blueprint plan for how to protect your team, and recommend you carry out an in-depth risk analysis of your project and data collection to understand where possible dangers to your team members lie and to develop appropriate contingency measures. This guide aims to support you through this process. There is a section including a list of suggested measures to minimize, counter and respond to risks which you can use as a point of departure and adapt, if appropriate, for your particular context. There are also links to other resources and organizations that have done in-depth work on this issue which can support your process of risk analysis and the creation of security plans.

We also encourage you to read our guide on digital security, which explores potential threats to the project data and suggests measures to increase the digital security of your project. These two guides are complementary and are meant to be used together.



What threats, dangers, and risks might affect you?

The safety issues that your team faces might depend on many factors, such as the degree to which the project is opposing the interests of other actors, the power/resources these actors have, the relationship you and the other actors have with the government, the restrictions or strength of legislative powers, the legal systems and treaties in place, the visibility of your project, the location of your project, and many others. They are also likely to change over time!

Listed below are some of the common risks and threats that might be helpful to keep in mind when carrying out a risk analysis with your team.

Targeted threats

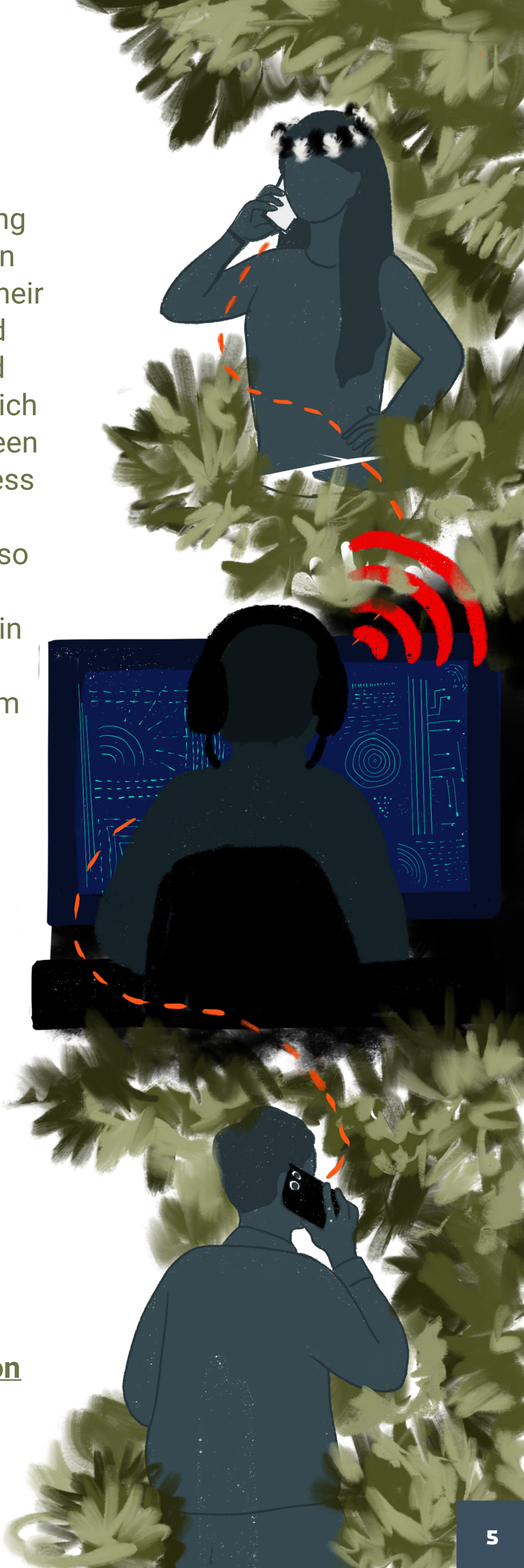
Earth defenders are often the target of groups with conflicting interests, meaning that the physical and psychological integrity of your team might be compromised at different moments of a project and in different ways. For example

- Criminalization - governments create laws that outlaw activities of earth defenders (eg. protests, visiting border areas, etc.) or create phony lawsuits to hinder your work or waste time.
- Unlawful detention including violence while in detention.
- Confiscation or theft of data and devices.
- Phone and device tapping/hacking/tracking to carry out surveillance on team members.
- Threats and intimidation to earth defenders and their families, which could lead to violence or even assassination.

DEFEND ENVIRONMENTAL DEFENDERS
STOP THE KILLING OF ENVIRONMENTAL ACTIVISTS
STOP CRIMINALIZATION OF EARTH DEFENDERS
EARTH DEFENDERS ARE NOT TERRORISTS

These situations might take place when earth defenders are collecting data in areas of conflict, but also in their offices, on the streets, or in their own homes, and their families and friends might also be involved and threatened. There are cases in which offices and private homes have been raided or burned down to get access to data and to spy, intimidate or harm earth defenders. We have also been told that on some occasions aggressors have set up traps within territories where conflicts are centered, aiming to physically harm earth defenders.

In addition to these dangers, the incorporation of digital tools in earth defenders' projects, whilst providing benefits for data collection, can also increase the ease with which governments, companies, and others track, follow, and collect information about earth defenders without their knowledge. This can expose earth defenders to new kinds of harassment. Conversations and protocols around digital security are therefore very relevant in these projects, and we strongly encourage you to read **the guide on digital security.**



Incidental dangers

Earth defenders face risks even when they are not specifically targeted by those with opposing interests. These risks may be related to carrying out fieldwork or gathering data in rural areas far from their communities, urban centers and other services. There might be the risk of getting lost; losing GPS or phone signal; running out of food, water or battery; getting ill or having accidents far from medical care. Equipment could also get damaged due to the environmental and weather conditions, or get lost or damaged due to fieldwork activities leading to potential data loss issues.

Other risks, not necessarily related to fieldwork include devices being stolen randomly, or data being lost through viruses. See the **guide on digital security** for other examples of incidental dangers and some suggested measures to minimize them.

Structural and environmental threats

It is also critical to understand threats arising from the local, regional or national contexts – those enforced by society, governments, or companies, and possibly based on racism, patriarchy, and other forms of oppression.

An example would be when a community is not included in decision-making around extractive industries despite the rights of Free, Prior and Informed Consent (FPIC), or if state departments turn a blind eye to companies using obsolete or polluting operational standards. Other risks might arise from environmental hazards and socio-economic dangers affecting earth defenders' communities. For example, only having access to polluted water, not having access to health services, or lacking hunting resources because of outsiders' overhunting.

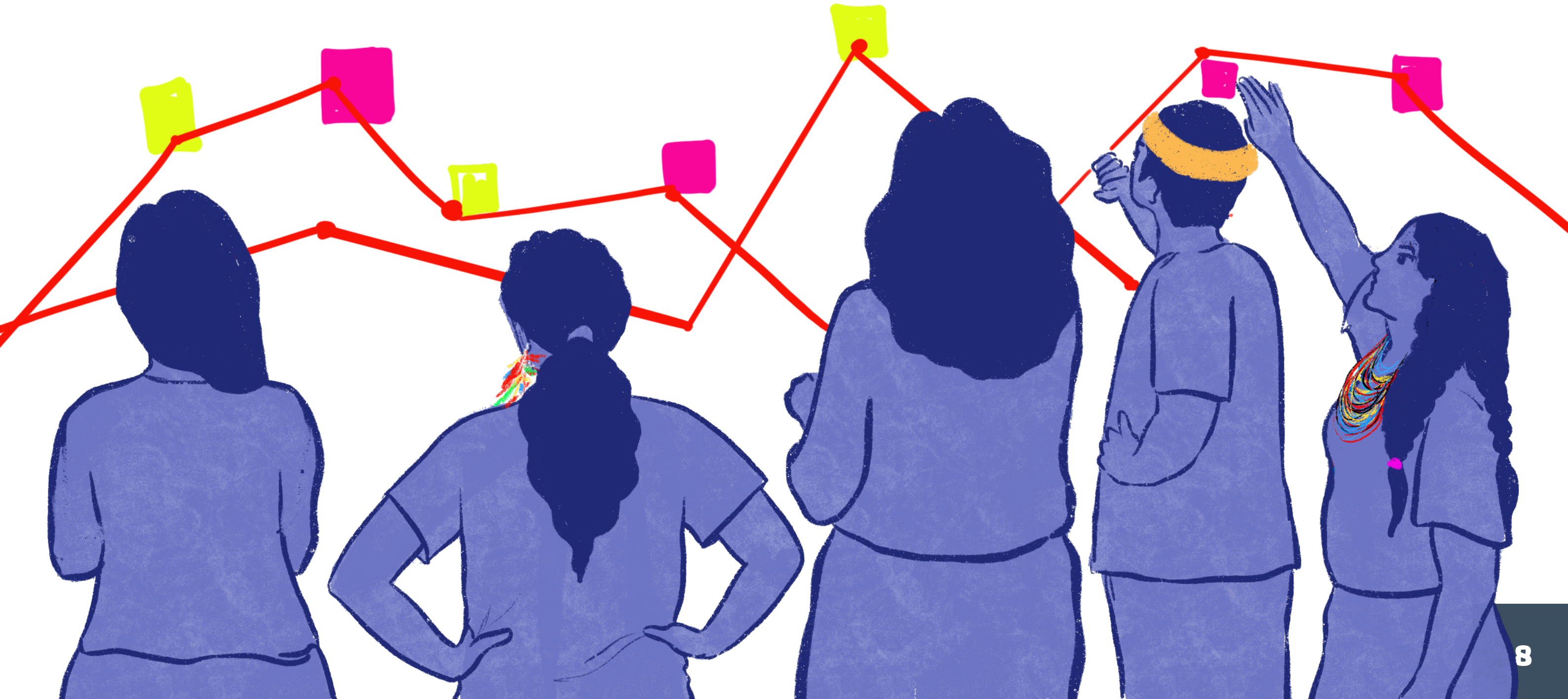
All these factors impact the personal safety of earth defenders and should be considered when carrying out a risk assessment.

Guiding questions and exercises

to do when considering digital security issues

This section proposes a selection of the exercises listed in the **Holistic Security platform**, a comprehensive and holistic manual to help human rights defenders maintain their well-being in action, the Protection International guide for human rights defenders **Taking Care of Us,** and the **Workbook on Security** from *Frontline Defenders*. We encourage you to visit their sites to access a more detailed and broader variety of exercises and resources.

We recommend carrying out these exercises with your team in order to ensure that the risk assessment includes all threats and dangers they perceive. Knowing how the team feels about things, and what measures they are already taking is crucial to designing appropriate safety protocols and rethinking aspects of the project as needed.



Broader picture

- Have there been any recent significant developments, including political, economic, social, technological, legal, and environmental, that might have an impact on the security and safety aspects of your work? Take into account the local, regional and international contexts.

Suggested exercises: Check out the **context analysis exercise** and **context questions** proposed by Frontline Defenders and the **PESTLE analysis** by Holistic Security.

Past and current risks, dangers, and threats

- What risks, threats, and dangers is your team exposed to? [We encourage you to read the **guide on personal and physical** safety to help with this question.]

For example:

- Physical - might impact the physical integrity of the team, their loved ones, their homes, buildings, and vehicles
- Psychological - might impact their psychological well-being
- Digital - might impact the information, equipment, and communication channels

- What have been the security and safety issues so far? Which patterns can be identified?

Note: also consider threats that arise from gender or race-based violence, from the political, social, environmental, and economic contexts, as not all threats are coming from groups whose interests are at odds with the work of earth defenders.

Evaluating risks, dangers, and threats

- Which are most likely to happen?
- Which would have the highest impact?
- What makes them feel more or less dangerous?
- How have you been communicating risks, dangers, and threats with your colleagues?
- Are there some situations that you consider too dangerous for you to work in?
- What security practices are already in place?
- What else can you do to minimize risks and threats?

Suggested exercises: Discuss with your team what they understand safety and security to be, and what they need to feel safe (which resources, activities, and help from people). Talk about which practices they already do to protect themselves on a regular basis and those that they have or would use in a dangerous situation. For more details, check this exercise by Holistic Security.

You can also carry out a **SWOT analysis** of your current security situation, covering the strengths, weaknesses, opportunities, and threats. Check these exercises on **Threat Brainstorm, Threat Perception,** and **Threat Inventory.**

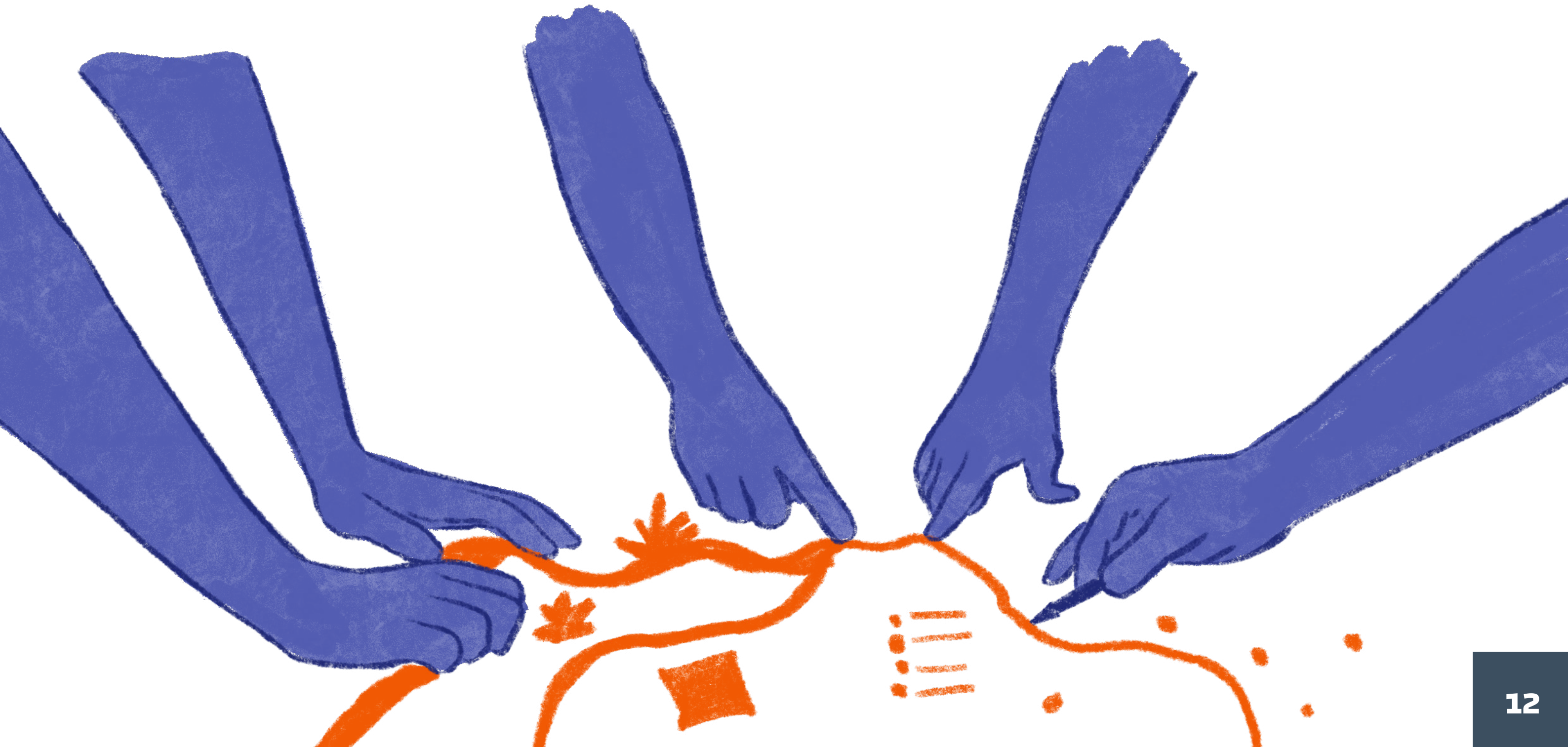
Mapping your information

- Are you collecting (or planning to collect) sensitive information?
- What would happen if your data were to fall into the wrong hands?
- What level of danger is there? Is it just about the loss of data or also malevolent use of it or even a threat to life?
- Is it worth collecting certain data given the associated risks? For example, do the benefits and added value of collecting detailed sensitive information such as the name of the person collecting data offset the generated risks?

Suggested exercises: Think about all the information that you and your team are collecting and producing – that means not only the products of your work (e.g. databases, reports, images, etc.), but also text messages, communications, and other office information. Where do you host the different information? With whom do you share it? Who can access it? Which software do you use for data storage, management, and sharing? How sensitive is it? For more details, check out the Information Ecosystem exercise by Holistic Security.

Mapping aggressors and allies

- Who are the actors with whom you have a relationship? Is this direct or indirect (or potential)?
- Who are your allies and potential allies - who can you ask for help?
- Who are your opponents, and potential opponents? - eg. who might stand to lose if your project is successful.

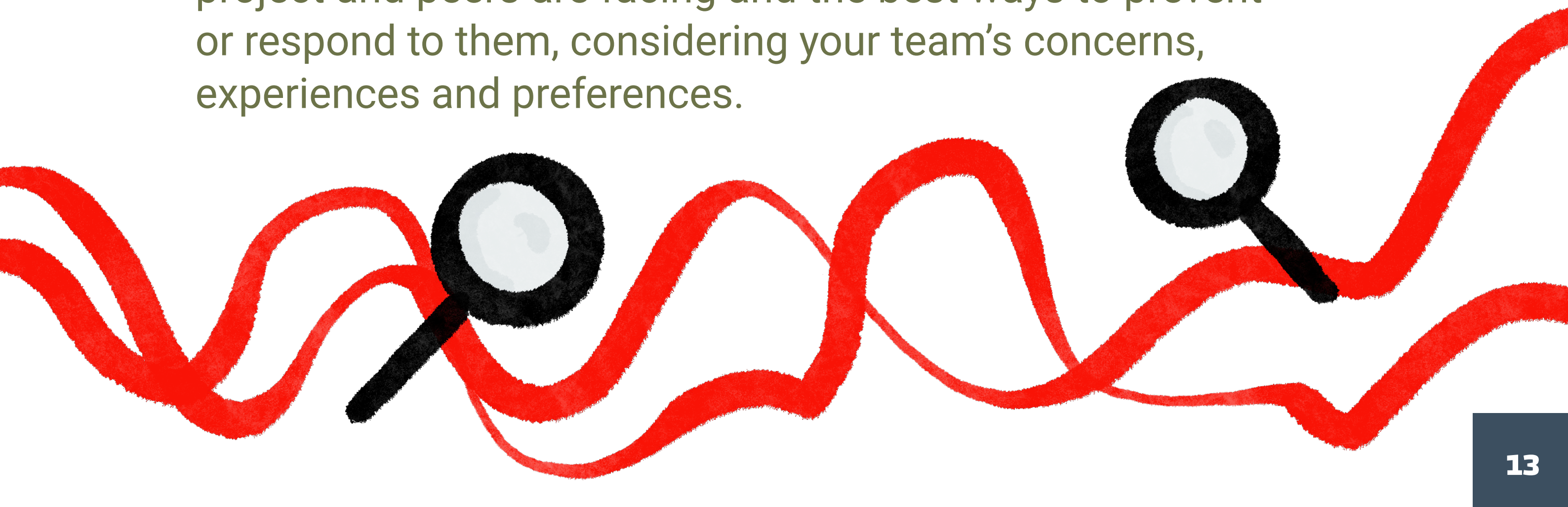


Measures to minimize, counter and respond to risks

Depending on the context of your project, it might be appropriate to put measures in place to minimize, counter and respond to personal and physical safety issues. See below for a list of suggested measures that you can use to pick from, and adapt those which might be useful to your project. **Drawing up appropriate security measures for a project requires a deep understanding of the threats, dangers, and risks** and the power and resources behind them, as well as a clear and holistic view of the big picture. Consult the Further resources section for a broader collection of exercises and digital security tips and suggestions.

Keep in mind that **threats, dangers, and risks evolve and change over time,** so it is a good practice to go over the previous questions and review your security guidelines on a regular basis and update what is needed.

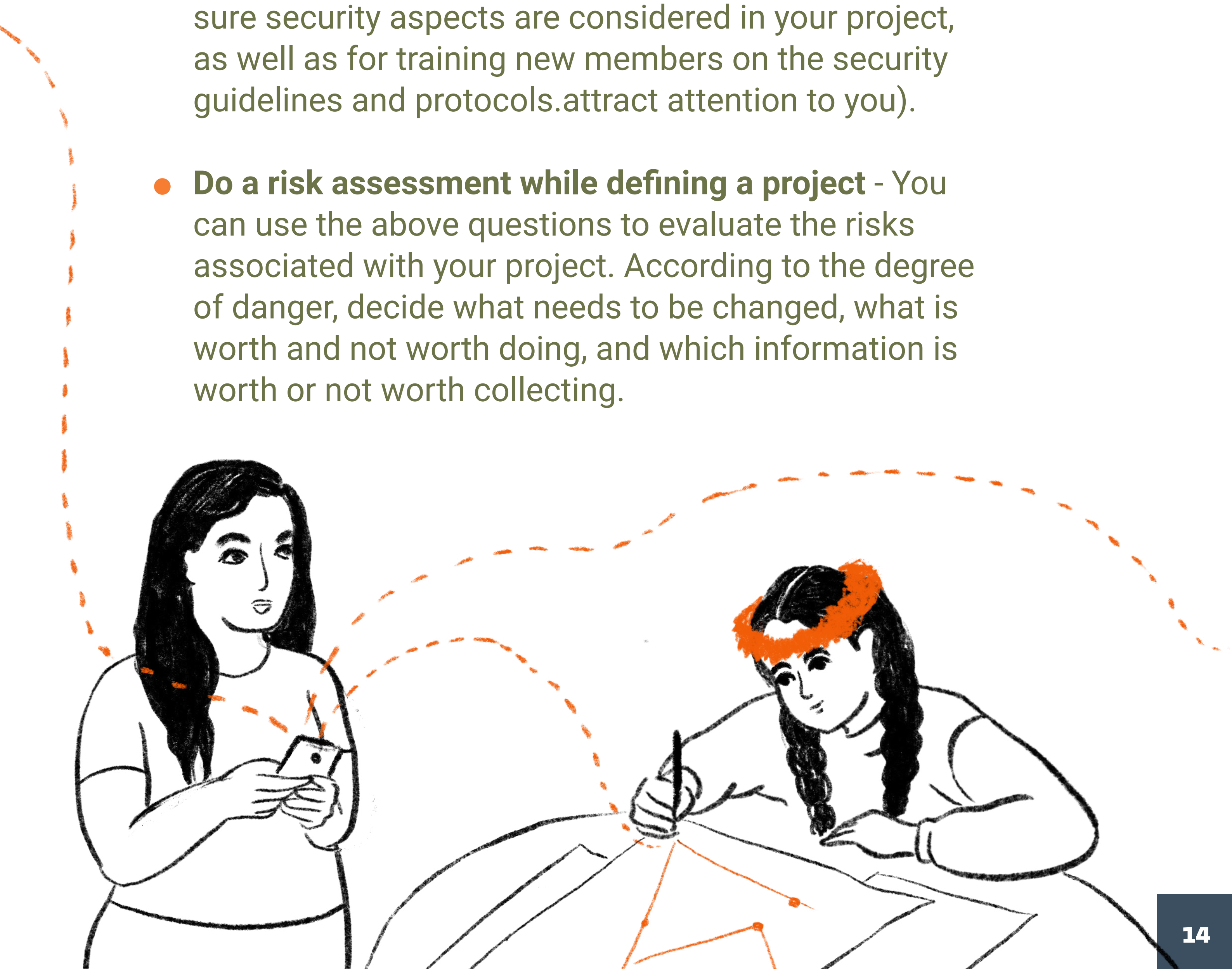
Finally, it is wise to **carry out these exercises as a team**. This way you will get a better sense of the security issues your project and peers are facing and the best ways to prevent or respond to them, considering your team's concerns, experiences and preferences.



Get informed and prepared in advance

- **Train yourself and your team on security concerns** –Get familiar with security and safety concerns that your project might face. Read guides on the topic, participate in training sessions on personal safety, digital security, etc. and **learn about your rights.** Check out this **checklist on capacities** that would help you decrease your vulnerabilities. There are different organizations that offer personalized security trainings, as well as long-term accompaniment, mentorship programs, and even helplines - check out the ***Further resources*** section for some examples. Consider having one or two team members be responsible for making sure security aspects are considered in your project, as well as for training new members on the security guidelines and protocols.attract attention to you).

- **Do a risk assessment while defining a project** - You can use the above questions to evaluate the risks associated with your project. According to the degree of danger, decide what needs to be changed, what is worth and not worth doing, and which information is worth or not worth collecting.



- **Create security guidelines and best practices for your organization**– Put in place strategies to minimize and counter risks and threats and create emergency protocols and keep them updated. Below we listed some suggested measures to increase personal safety, but you need to evaluate their pros and cons and assess if they are appropriate for your project. Check out this **guide on digital security** for complementary measures. We also encourage you to visit the guides listed in Further resources, especially the **Workbook on Security** by Frontline Defenders, which provides the steps needed for the creation of a security plan.

Minimize risks to earth defenders

- **Put in place spaces for talking about safety:** During the whole project, it is important that participants have a space to talk about the threats they perceive, and the level of danger associated with them. Having mechanisms and protocols on how to communicate risks will not only help the team to be aware and prepared, and keep the security plan updated but might also help deal with the **emotional load and stress** and create a support network.

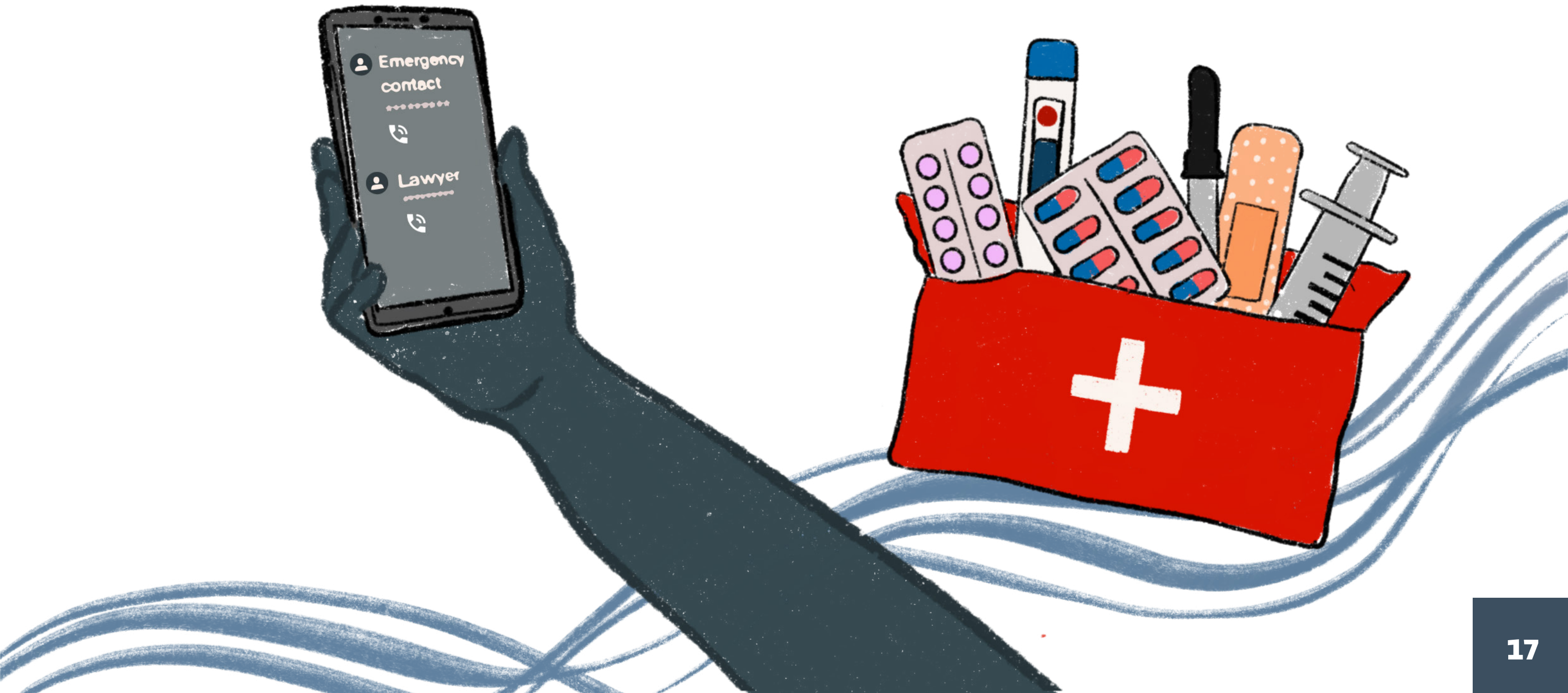
- **Get ready in advance :** Do risk assessments before trips if risks are expected to be high and make sure everyone is trained on security and safety aspects and how to approach different scenarios. There are different organizations (see ***Further resources*** section) that offer personalized security trainings and grants to address emergencies.

- **Minimize risks when visiting dangerous sites:** A general recommendation is to go in groups and avoid traveling after dark. Bring with you a first aid kit adapted to the local threats and have the team be trained to use it. Carry maps (offline and/or on paper), GPS devices, compasses, or any tool to minimize the risk of getting lost. If available, take a satellite phone for emergencies, as well as emergency contact numbers on the top of your contacts list on your phone. Wear comfortable shoes and keep in mind that you might need to run. Take a look at these **additional considerations for traveling**. In risky situations, hide your devices (e.g. GPS, phone, drones, etc.). If you need to use them, do it from afar and carefully. Consider using an alias name. If the risks are very high, take as many precautions as possible, consider asking for support from police, government, or non-governmental groups, and consider not doing field visits if risks are high.

- **Discuss the responses to risks and make an emergency plan:** Make sure to include what you consider to be an emergency, what everyone's different roles will be, and which communication channels will be used. Train the team on this strategy so that everyone is on the same page. Consider using a whistle. There are apps and gadgets that send a signal when you or your team are experiencing a threat. Contemplate getting in contact with organizations that offer support and grants to address emergencies (see ***Further resources*** section).

- **Have a plan around dealing with surveillance if appropriate:** As explained in the **guide on digital security,** many devices can easily be tracked and tapped and in the guide, we listed some measures you can take to minimize vulnerabilities. If you think you could be under surveillance, read these **suggestions and best practices** from Frontline Defenders, which include considerations for both dealing with surveillance technology (such as microphones, cameras, etc.) and physical surveillance. A general suggestion included is to always assume you are under surveillance even if you are not sure about it.

- **Contemplate the risks of arrest, kidnap and abduction if appropriate:** If you are at risk of being arrested, abducted, or kidnaped ask for support and advice from people with expertise in this area and check out these **recommendations** from Frontline Defenders. Some examples they list are, if being arrested is a possibility, carry any necessary medication at all times, and have the contact details of a known lawyer (learn their telephone number by heart).



- **Minimize risks in the office and at home:** Consider using the checklists from Frontline Defenders on suggested measures to increase security in the **office** and at **home**. Examples include having an emergency contacts list with useful telephone numbers and addresses (e.g. local NGOs, hospitals, police, ambulance, etc.); using protection measures (e.g. locks, bars, gates, fences, alarms, good lighting around the house) while trying to match the measures used in the neighborhood to avoid creating suspicion; having key procedures and replacing keys when stolen or lost; having a plan in case the office/home is raided; having protocols for when someone leaves the project or having a code word or sentence for emergencies.

- Spotlight the threats and seek external help: If needed, approach international organizations, special rapporteurs, and powerful actors working on human rights defenders, and ask for their accompaniment and support. Consider using media and social media channels to amplify the issue and put pressure and visibility on the threats that you are facing, but first, assess all the implications and consequences of spotlighting yourself and the project in the media. Also, have a plan on how to deal with trolls on social media. Check out this guide from Security in-a-box to **protect yourself and your data when using social media** and take a look at these measures suggested by Frontline Defenders **in case of defamation.**

- **Reduce unintended and accidental personal dangers:** Carry a first aid kit adapted to the local threats and have the team be trained to use it. Carry maps (offline and/or on paper), GPS devices, compasses, or any tool to minimize the risk of getting lost. If available, carry a satellite phone for emergencies, as well as emergency contact numbers. Consider taking out medical insurance.

Improving your digital security

Strengthening digital security is fundamental and is deeply interlinked with the personal safety of earth defenders. In the **guide on digital security,** we have compiled a variety of potential measures to limit access to your devices and data, prevent and identify remote and physical intrusions to your device, track data edits, prioritize safe apps and networks, and have protocols around data backup, sharing and syncing.

Further resources:

Other personal and physical safety guides

- Check out the **Workbook on Security** by Frontline Defenders, which takes you through the steps to a security plan, and develop risk and vulnerability reduction strategies. Available in 10 languages.

- Take a look at the manual **Protect against physical threats,** from Security in-a-box, to get more measures to increase the security of your team. It is available in 17 languages, including **Spanish, Portuguese,** and many others.

- **Security in-a-box** also offers multilingual manuals on relevant topics such as using safe passwords, communication and browsing channels, protecting devices from malware and phishing and managing sensitive data.

- Visit the **Holistic security** website. It is a very complete and comprehensive platform with multiple exercises, an holistic approach to security. Many of the exercises featured in this guide are inspired by theirs. Only available in English.

- Check out this **Trainers' manual** on security and well-being for human rights defenders by Holistic Security.

- Read the guide **Taking Care of Us - A Guide for the Collective Protection of Human Rights Defenders in Rural Areas**, by Protection International. It is available in English, Spanish and French and it includes multiple exercises. Chapter 2 features a threat analysis and exercises to identify aggressors and allies.

- Consider reading this report on **Organizational Security Community: Challenges and Opportunities** by The Engine Room and their **report addressed to digital rights funders**, which among other things, encourages centering safety and protection in funding approaches, as part of creating sustainable movements.

- Take a look at a summary of the **list of rights that are fundamental to environmental defenders** or **The Living Convention** by Natural Justice, for a more extended list of rights.

- Want to check out other guides? Take a look at this **list of resources** compiled by Holistic Security.

Useful exercises

The exercises listed in this guide have been inspired by some of the exercises featured in:

- The **Holistic Security** exercises summary
- The **Taking Care of Us** guide by Protection International, especially chapter 2
- The **Workbook on Security** from Frontline Defenders

We encourage you to visit their sites in order to access more detailed and a broader variety of proposed exercises and workshops.

Recommended articles

- Read **Last line of defense,** the key findings from Global Witness on their analysis of the killings of land and environmental defenders.
- Watch this segment on Democracy Now on **the Dakota Pipeline Company's bulldozing of sacred sites after a Sioux map was made public.**
- Take a look at the article **Protecting the Defenders: Exploring the Role of Global Corporations and Treaties** by Ian Granit.
- This recent piece by Albertine Watchdog exposes **many examples of targeted threats and intimidation of environmental human rights defenders**

Getting support

Take a look at this **compilation of support contacts and resources** by Holistic Security, featuring existing Emergency Grants, Fellowships, Scholarships, Rest and Respite and Awards for Human Rights Defenders.

The UN Special Rapporteur on Human Rights Defenders has prepared a **list of organizations and resources to support defenders in different ways,** from security and legal support to relocation and emergency protection.

Frontline Defenders also created a **compilation of organizations providing support to defenders.**

Helplines

The **Access Now Digital Security Helpline,** with a 24/7 multilingual service.

The **Feminist Helplines,** which provides support to women and LGTBQIA+ people facing digital gender-based violence.