HOW TO ORGANIZE A DIRECT ACTION?

AGAINST THE ZIONIST WAR MACHINE:

A PRACTICAL FIELD GUIDE

WELCOME

Welcome and thank you for being here. This practical field guide serves as a tool to help you organize your own **direct action against the Zionist war machine** in Belgium. Read this manual carefully and good luck.

IMPORTANT NOTES ON DIGITAL SECURITY:

Digital security basics:
→ Always use a Tor browser,
→ Do all your research with a VPN
→ Have proper passwords on the tools you use, that are never automatically saved on your computer (memorize them!).

And even more important regarding security:
Do not boast about what you plan to do or have done. Do not discuss it in bars or at parties, even if you seem to be among friends. Call each other out if you see this happening.

STEP 1 - FORM AN AFFINITY GROUP

An affinity group is an autonomous group that takes action. It is crucial that you only invite people you know well and trust to become part of your affinity group. The smaller the group, the safer: 4 to 8 people is an ideal number, but some actions can also be carried out with 2 or 3 people.

Once you have formed a group, come up with a name. You could use the name of a Palestinian freedom fighter, a play on words or something else that is appropriate.

You communicate with each other via Signal. Carefully read the digital security guidelines and the end of this manual to use Signal in a safe way.

Next, get a Proton email address or another encrypted address. This is crucial for sending information about your action to Stop Arming Israel.

More on this later in this guide.

STEP 2 - CHOOSE A TARGET

Now that you have your group, choose a target.

Go to **www.stop-arming-israel-belgium.com** for a list of companies linked to OIP/Elbit or in another way involved in the production or transit of military equipment from Belgium to Israel. This list is regularly updated!

All of these targets are complicit in genocide. By sufficiently increasing the costs of their cooperation with the Israeli war industry through our actions, we force them to reconsider their cooperation with the Israeli arms industry.

When choosing your target, take into account where you live to simplify planning and scouting and save on transport costs.

Are you based in France? Here you will find a (non-exhaustive) map with more than 170 sites of French arms manufacturers complicit with Israel.

STEP 3 - PREPARE FOR ACTION

1. SCOUTING

When preparing for an action, it is essential to know your target well and to scout it out. Do this as discreetly as possible so that you are not caught on the spot or identified after your action. How you should behave depends on where your target is.

Make sure your phone is always on flight mode while scouting so you can not be identified afterwards via your phone signal.

If your target is in the city centre, there is nothing suspicious about taking a walk with a friend or alone and taking out a camera to photograph the location. But if you walk around an industrial area with a selfie stick, you are likely to attract attention.

If you are going to locations in more rural areas, try to take a dog with you for a walk. Or put on sportswear and go running or cycling. Make sure you have a convincing story why you are there in case anyone asks you (looking for a lost cat, geocaching etc...)

You can also scout with a car, but make sure you only drive by once and gather all the information you need in that one trip so that your number plate does not appear on camera multiple times.

When you go scouting, it is good to take pictures but be aware of the following:
- Take pictures directly in Signal. In that way they don't leave any digital traces on your phone. Remember: keep your phone on flight mode. The pictures will be sent as soon as you have connection again.
- Don't attract unwanted attention by taking pictures or videos. Be quick or keep your phone in a position in which it is not obvious that you are taking pictures. You can for instance walk, cycle or drive past the target while you phone is filming, in stead of standing still. Or pretend to take a picture of something else with the target in the background.

If you do your scouting long before the action, plan a second scouting trip just before to check if there is any important changes on site.

2. ONLINE RESEARCH

Before you go to the city center or walk your dog, it is always worth scouting online first. This will give you a better idea of what you could do during your action and what you need to find out during your scouting mission, without taking too many risks.

In addition to Google Maps, use Google Earth or maps such as Bing and Mapillary, which sometimes provide additional information. If possible, do this with a secure browser and VPN. Google Maps often does not work with Tor, but make sure you use a browser where you are not logged into Google!

Do not rely solely on online information, as companies are constantly changing things and online maps are not always up to date. Nothing beats a personal visit to prepare yourself properly.

Important information to find out

- **Security guards** - How many security guards? Stationary or moving? Inside or outside? What are they watching? What can they see? Which street? What are their schedules - it is better to avoid the times when they change shifts, as there will be more security guards on site then. Do the security teams stay within the site or do they try to guard entrances from outside?

- **Workers** - How many people seem to work at the location? Can you count cars? What are the working hours? Is there moments a lot of people leave or enter the building? Do they work 24/7?

- **Cameras** - Positions? Number of cameras? What are they focused on, what can they see? It is often not possible to take action outside the view of cameras, so it is crucial to be anonymous and unidentifiable.

- **Entrances** - How many access points are there to a site or building? Also pay attention to emergency exits. What kind of locks are on the doors and how can you open them if necessary?

- **Surroundings** - What is in the vicinity of the target? Neighbors or other locations? Do the surrounding buildings have security guards? Or at what times of the day are there people present in the surrounding buildings?

- **Alarms** - Is there an alarm? What could trigger an alarm? Anything that could activate an alarm should be done last.

- **Police** - Where are the nearest police stations? Is the area patrolled? At specific times? Are there undercover cars in the area? Foot patrols? Estimate the response time of the police.

- **Parking** - Where to park before, after and during the action. It is important to find parking spaces that are not monitored by cameras and do not require a parking ticket.

- **Transport** - Can you get to the location by public transport? Are there places without cameras (a park, an open field) where you could change so you won't be spotted on cameras in transport?

- **Exit plan** - How can you leave the location without being seen on camera? Are there cycle paths, fields or woods where you can disappear without being followed? Are there public spaces (stations, shopping centres) where you can blend in with the crowd? Make sure you have multiple exit plans.

3. SET UP A LEGAL SUPPORT TEAM

Why have a legal support team?
The purpose of a legal support team is to ensure that activists who are arrested or prosecuted are not left to fend for themselves and that their rights are respected. In addition, a legal support team serves to maintain an overview, inform friends and family if necessary, and organise support campaigns, crowdfunding, and communication.

How do I organise legal support?
Depending on the action, the experience or the needs of the activists, your legal support can be as small or as large as you want. Below is a detailed step-by-step plan of the possibilities, but this will certainly not be necessary for every action. A minimal version is that someone outside the action is aware that you are going to take action and checks whether you are home within 24 hours and informs the necessary persons.

For a smaller action, a legal support team can consist of one or two people who stay at home or in a safe location and follow the action. The purpose of legal support is to be well prepared before, after and during the action for any legal consequences and the emotional stress that this may entail.

STEP 4 - PLAN YOUR ACTION

1. TYPES OF ACTIONS

Now that you have done your scouting, it is time to develop and refine your plan. Creativity is very important to keep our resistance effective. When preparing your action, it is a good idea to clearly define with your group what you want to achieve with your action.

Here are a few examples of how different direct action groups for Palestine have already done this. If you have little experience, it is best to start with simple actions and gradually move on to more complex ones. All ideas that fall within the action consensus are possible. Here are some suggested tactics to get you started...

- **Redecorate your target:** Fire extinguishers can be hacked and filled with blood-red paint, spewing large amounts of paint when activated. This allows you to cover large areas with paint in no time. Perfect for quick action.
- **Paint your message:** Tagging with spray paint can also be quick, as long as you don't try to write a long story on the walls of your target.
- **Block the target:** You can block entrances of a building before people arrive at work, so they can't carry out their activities. Or block trucks with necessary materials from going in or out of the locations. Blocking can be done with your body (but high chance of getting arrested and potentially identified) or with materials; a bike lock around a fence, a big hole in the road so trucks cannot pass, glue in the locks of doors etc.
- **Use your imagination anything is possible ;)**

Think big: The tactics given here are examples of actions that have already been taken, so don't be afraid to try something new! Don't limit yourself to what already exists, but ask yourself every time you brainstorm: what could I do to be more creative?

2. PREPARE FOR THE LEGAL CONSEQUENCES

Assess and inform about the risks
Based on your action plan, you can assess the legal risks you may be taking. To do so, you can refer to the legal risks document and the criminal code, among other sources. If you have specific questions, you can also contact the Stop Arming Israel Belgium legal team. The legal team consists of people with experience in activism and legal teams, but not necessarily solicitors or lawyers. They will provide you with the best possible information.

Discuss this within your group and evaluate together whether the expected impact is worth the risks and whether everyone feels comfortable with it.

LET'S GOOOOO...

Action consensus

Discuss whether there is a need within your group to draw up an action framework and agree on how far you want to go with the action (what feels comfortable and what does not).

Read the action consensus of Stop Arming Israel Belgium and discuss whether you agree with it.

Practical preparation:

- Ensure you have a lawyer or a list of lawyers you trust who can provide legal support in the event of arrest and/or prosecution.
- Decide how activists can contact you during the action. Bear in mind that this must be possible from the police station. It is strongly recommended to use an anonymous number on a phone that has never been used before and that operates from an anonymous location. You can also agree that, in the event of arrest, activists will contact a family member or friend who is not involved in the action and who will then contact your legal support team via Signal.
- Choose a location from which the legal support team will follow the action. Keep in mind that if you want to be reachable by phone, you must choose a location that is publicly accessible so that an investigation into the phone records (phone mast connection) cannot implicate anyone in what you are doing.

Information and agreements with activists:

- Make a list of all persons at risk of arrest. Ensure you do this for everyone, including scouts or persons who only bring materials or drive activists.
- Collect the following information:
  - Who to contact in case of arrest or if something goes wrong, and after how long and with what message (e.g. after 24 hours, call sister to call in sick, call housemates).
  - Important medical information (e.g. cannot go 24 hours without psychiatric medication).
  - Information about other legal proceedings (residence proceedings, etc.) and lawyers.
  - Make clear arrangements about where people will meet up after the action and/or arrest and how the legal support team will be informed.
- Encourage activists to choose a clear "nest" or meeting place where people can find each other if you lose each other or if you are released during the night. Agree on how long you will stay there and when you will move to another location.

Anticipate arrest locations

Based on the location of the action, you can already anticipate where people might be taken in the event of arrests. Do you know people who live nearby where activists can go if they are released?

2. HOW TO REACH THE SITE AND LEAVE UNDETECTED

Transport is an important part of any plan and can make the difference between getting away with it and getting caught. Here are some examples of different means of transport and how you can use them to your advantage:

- Walking to a location can be very effective. The key here is to keep your face covered at all times and find a place where there are no cameras to change into different clothes and continue on your way. Try to find a busy place to change, such as a shopping center, or a place with many different exits, such as a park, so that you cannot be easily traced later on camera.
- By bicycle. Bicycles are great for covert operations. Park your bicycle somewhere near your target, but in a place where there are no cameras. Then walk from that point to carry out the operation and return to your bicycle. Make sure your bicycle is not easily recognizable on camera footage and, if necessary, borrow a neutral bicycle so you don't have to use your everyday bicycle covered in activist stickers.
- A car is sometimes the easiest way to get around. But they have number plates that can be picked up by cameras and traced back to the owner. If you plan to use a car, make sure you know where all the cameras are located on the route you want to take - and find a route that avoids them completely. Do not park the car next to the premises, but in a place out of sight of cameras.
- If you use public transport, do NOT use your own debit card or Mobib card. This information is stored and can be easily accessed by the police. It is always best to use cash. Nowadays, however, many forms of transport do not accept cash payments. If you are in Brussels, it is best to use an anonymous Mobib card that you have topped up with cash. On the train, use a ticket from the ticket machine that you have purchased with cash. Be aware that public transport is full of cameras, so keep your face covered. However, boarding a bus or train wearing a balaclava may arouse suspicion. So think of other ways to cover your face – face masks have become commonplace since COVID, and you can also wear sunglasses.

The route. When choosing your mode of transport, make sure you have carefully considered all your routes to ensure a perfect escape. Think about the positions of the cameras and don't take off your face mask too quickly. If the police really want to find you, they will follow you on camera to the place where you took off your mask and get a picture of your face. Wearing a cap increases the chance of hiding your face, but there are no guarantees. It is best to remain masked until you are in a safe place, where there are no cameras and it is relatively busy. From there, you can plan your route home.

3. ROLES

If more than one person is involved in the action, you need to divide the roles. For example, if you want one person to focus solely on taking photos and videos, then he or she should focus on that and not on waving paint around! The others can spread out across different parts of the site, or one person can work with paint another with something else 😉

Whatever your action is, make sure you have decided who does what to make the action as efficient and quick as possible. That is exactly why it is so important to plan your action well, so that everyone knows what they are doing.

Outside support - ensure that one or two individuals who are not participating in the action are aware of your plans. You should contact this person once you are safely home. This person does not need to know all the details, but should have instructions on what to do if you are arrested (call a lawyer, feed your cat, call your work to report sick, etc.). Make sure this person has all relevant information, including the name and phone number of a lawyer.

3. MATERIALS

Now that you have worked out your plan down to the last detail, it is time to purchase materials. At this point, it is a good idea to remember that CASH IS KING. When purchasing materials, whether paint sprayers or other stuff, do not leave any paper or digital traces behind. Use cash and wear a cap in the shop and/or a face covering, just to be on the safe side. But don't behave too suspicious. You can also ask a friend that won't participate in the action to go shopping for you. And you can buy your materials in different stores.

The materials you need will depend on the type of action you are going to take. These could include paint sprayers, fire extinguishers filled with paint and hammers. Don't forget to wear safety gloves and safety classes: you don't want to cut yourself and leave your fingerprints or blood at the scene!

If you would like advice on equipment, for example how to fill a fire extinguisher with paint, please contact us via e-mail: contact@stop-arming-israel-belgium.com or via Signal if you have already a direct contact.
Important: never leave any material behind after your action. Absolutely nothing except paint. The police may try to conduct forensic investigations into any objects left behind in order to trace who was involved in the action.

4. CLOTHES

- Face coverings are most important. Ensure that your face is not visible at any point during the action. A balaclava is best for this, but you can also use a cap, face mask, and sunglasses. If you normally wear glasses, try to find another solution (contact lenses, your old glasses, no glasses).
- Wear "normal" shoes that do not stand out. Do not wear shoes that you wore when you were arrested during an action or protest, or that you wear in photos on social media. It is best to buy the most ordinary, boring black shoes and only wear them during an action.
- Wear dark clothing (preferably black) that is not conspicuous. Wear loose-fitting clothing. This makes it more difficult to determine your posture.
- Cover your entire body. This is especially important if you have recognizable features such as tattoos or moles. Therefore, make sure you have gloves as mentioned above and that everything is covered.
- Wear clothing that you are willing to throw away after the action.

STEP 5 - THE ACTION

Adrenaline will be pumping through your body and your nerves will be tested at the same time. This is normal. Make sure you go over your plans again before you take action, to ensure that everything is clear to everyone.

Delete Signal from your phone and laptop to not leave any traces in case your house is searched afterwards. Make sure your computer is not logged in to any tools you used in preparation. And throw away any physical evidence like papers with notes on it.

Go for it! It's the day, you've planned your action well, you're rested and you're ready. Good luck!

1. DOCUMENT YOUR ACTION

The main goal of your action is to cause economic damage and thus exert pressure. However, do not underestimate the power of communication so that the message is spread further. This way, other potential targets can see what awaits them, it can inspire other groups to take action, and more importantly, the people in Palestine know that our solidarity is being translated into action.

Resources

- Download a logo from our campaign on our website
- Read more about Elbit and campaigns targeting it on our website
- Free design softwares to edit videos and/or images: Canva (online), Inkscape (offline), Gimp (offline), Premiere Pro (offline). If working online, always check the digital security guidelines. Be careful of "offline" softwares that automatically upload data online.

Digital security

- **Carefully read the digital security guidelines at the end of this handbook.**
- NEVER take your own phone to an action as it can be traced to you. Ideally, give your phone to a friend to take it out for a walk in places without a camera (like parks) so you create evidence that your were not at the location of the action.
- To document your action on video or photos, buy a cheap second-hand smartphone. Pay it with cash. For more info on have to safely use this burner phone, read the digital security guidelines at the end of this document.
- When filming or taking pictures, make sure no one is identifiable. Cut footage where people are identifiable or send clear instructions for editing.

Writing a press release

- Start with a short summary of the essential details in the first paragraph using the five W's: who, what, when, where and why.
- Be concise: keep your press release short.
- Be relevant: Tell your audience why they should care.
- Be structured: Use clear titles to introduce paragraphs to help the journalist read the text quickly.
- Describe your action objectively, and put political, "subjective" text in quotation marks. For ex: X said, "This company is guilty of genocide" (so the journalists can publish your text directly).
- Include one paragraph with more general context on the campaign and/or the company to situate your action for journalists.
- Send us your press release or send it yourself from a safe email account if you have a press list already!

Social media

- You can send us materials to post on our social media account. We can also collaborate on posts if you'd like to use your own account.
- The posts that do best are short videos (2-3 mn). Try to start with the most impressive images to capture people's attention. Music can be added to the post via Instagram directly.
- Otherwise, prepare a series of images for a carrousel post, with explanatory text.
- Please send us your caption for your photos / video, preferably in Dutch and French. We usually save English for main posts.

Sending us your materials

Please read the action consensus to know what we will and will not publish on our social media and website.

Remove metadata from your files before sending them. This is all data that may contain identifiable information. Clean up your files on your (crypted) computer by using Metadata Cleaner (https://metadata.systemli.org/).

To send your press release, images and videos of your action safely, we recommend you create a folder on an anonymous cryptdrive using a VPN + TOR. You can create a cryptdrive here: https://cryptpad.fr/

You can send the link to this folder via an anonymous Proton email address (with a VPN) to our Proton email address: stop-arming-israel-belgium@proton.me (emails between Proton addresses are encrypted).

2. WHAT IF THINGS GO WRONG?

You provide support from a distance for your comrades during the action. This means that you record and follow up on the action and any arrests that may occur, and provide physical and emotional support as much as possible.

Registration:
- Record the time your comrades were arrested, if you have this information.
- Keep an eye on whether they are being detained for too long.

Follow-up for the first 24 to 48 hours:
As long as the arrested person is in administrative detention or has not yet been questioned in the case of a judicial arrest, the focus is mainly on support and care. From a legal point of view, not much can be done at that stage. As long as there has been no questioning, a lawyer has not been officially appointed. At that point, therefore, they cannot do anything.

In the case of a judicial arrest, an interrogation may take place. At that point, the arrested persons can provide the name of a lawyer who must be contacted by the police. That is when it may be useful to contact the lawyer (if you know who has been appointed). The lawyer can inform you about the status of the arrest, the location of the detention, etc.

- Call the contact persons you would inform if this had been agreed.
- If necessary, call police stations (or hospitals) if you do not have any information about where the arrested persons are being held. Think carefully about the number you are calling with. It may be safer to ask someone who is close to the persons and has nothing to do with the action to make the call.
- Stick to the agreements made with the activists.
- Lawyers cannot really help with this because the person is not yet officially a client at that point.

Follow-up in the event of prolonged detention:
If a person is still being detained after 48 hours or after meeting with an investigating judge, there is a good chance that the investigating judge has issued an arrest warrant. This means that the person can be detained for longer and will be transferred to prison.

If someone remains anonymous, it is also possible that the person will be transferred to a closed detention centre on the pretext that they do not have any papers.

- Contact the legal team at Stop Arming Israel Belgium.
- Find a lawyer who can follow up on the case.
- Discuss with the lawyer whether it would be useful to communicate publicly about the situation.
- Consider organising protests at the police station/prison/detention centre
- If someone has been sent to a closed centre and does not have Belgian nationality, it is important to contact the lawyer who is following the residence procedure.

Aftercare / Arrestee support:
- Ensure that your comrade(s) is/are met at the police station or the agreed meeting place. It is really valuable for people to be met when they leave the police station. Often, people do not have a telephone and need someone to talk to, so it can make a big difference for someone to be waiting for them.
- Bring coffee, tea or biscuits (or something else).
- Listen to their stories / Be available / Do something nice.

STEP 6 - AFTER THE ACTION

1. ERASE ALL TRACES

You have just disrupted a company that is complicit in genocide. At this point, you want to make sure you destroy all evidence. If you have any empty spray cans or other items, dispose of them as soon as possible, after cleaning them in case you touched them without gloves.

- Do not put them in the bin at home, but find a public place to throw them away. If you do not want to get rid of your clothes, make sure they are not at your home or in your car. Take them to a friend's house.
- This all may seem excessive, but it is very reassuring to know that no evidence remains at the location or in your home. If the police ever get to the point of searching your home (which is very unlikely if you follow all the steps above), they will look for items that connect you to the act.

Don't forget to:

- Send your footage to the Stop Arming Israel Belgium campaign: contact@stop-arming-israel-belgium.com
- Delete all photos from the burner smartphone.
- Remove metadata from all compromising files.
- Edit anything that could reveal your identity in the photos/videos (voices, faces, etc.).

In addition to the photos and videos, you can also send us your own press release, which we will forward to journalists together with your campaign.

2. MONITORING LEGAL CONSEQUENCES.

Ensure legal follow-up and monitor repression.

- Send the legal team of Stop Arming Israel Belgium a brief debriefing of what happened, if necessary.
- Stay in touch with your comrades and keep each other informed of legal consequences. Remain united and support each other in legal matters.
- Contact the Stop Arming Israel Belgium legal team to assist you with any legal proceedings.

SÉCURITÉ NUMÉRIQUE

Foreword:
This manual aims to introduce good digital security practices without going into technical details. For more rigorous and comprehensive guides, see:
https://activisthandbook.org/tools/security
https://www.frontlinedefenders.org/en/digital-security-resources
https://technopolice.be/autodefense-numerique/ (in french)

1. BASIC PRECAUTIONS

ANY activity on an electronic device leaves traces that can be exploited by skilled individuals.

Tip number 1: Avoid any unnecessary actions. Example: do not download files from the cloud, even if you do not like working online, as this will leave traces on your device.

Tip number 2: always take precautions. Use a pseudonym in real life and fake names on the internet. Do not put all your information in one place, do not link your accounts, data and spaces together.

Tip number 3: Don't go too fast. These basic tips should always be followed. You can use technical tools to project yourself, but they should never replace basic security principles
.

Tip number 4: Security is collective. If one person in a group takes security lightly, that person can serve as an access point and compromise the security of the entire group.

During a meeting
Do not discuss sensitive matters with people who do not need to know about it.
Collect all phones and put them away in another room.
If you need a computer, use an encrypted one and, if you need to connect to the internet, use a VPN and TOR (detailed explanation below).
Ask everyone to activate their aeroplane mode well before arriving (a few kilometres from the venue). This will prevent telephone operators from proving that you were all together (collective geolocation and triangulation).
Change venues for each meeting.

Outside of meetings
If people don't need to know, don't tell them anything. Don't say that you are involved in organising a particular action. This also applies to your family members and close friends.
If it is comrades who need information about the action, give them only what they need to know for their role.
If you have to go somwhere for sensitive activities such as a scouting missing, activate airplane mode. Ideally, activate it regularly at random for random periods of time to cover your tracks.

2. COMPUTER

Avoid using your phone as much as possible for searches related to an action (maps, location tracking, internet information, etc.). Do your research on a computer using a VPN+TOR.

As much as possible, do not save sensitive documents. Encrypt your computer. The user password does not protect much.

Deleting a document on a computer or USB stick does not actually delete it and it is possible to recover it. To delete a file on a disk (hard drive, USB stick, SD card, etc.), you must overwrite the data and format it.

Encryption

Encrypting data means transforming it so that it can only be read by authorised persons. To access the contents of an encrypted disk, you need to have the 'key', for example a password.

There are two main precautions to take into account:
The computer is only encrypted when it is turned off, so turn it off, don't just leave it on standby.

The strength of the encryption depends on the strength of the password you choose, so make sure it is long (20+ characters) and ideally a random mix of lowercase letters, uppercase letters, numbers and special symbols.

How to encrypt your computer

It is best to avoid using the native encryption programme that comes with your computer, such as Windows' BitLocker encryption option. We don't particularly want to trust Microsoft. Here are our recommendations:
For a Linux computer, it is possible to encrypt the disk when installing Linux using the LUKS specification. More details for Ubuntu, for example: https://documentation.ubuntu.com/security/security-features/storage/encryption-full-disk/
For Windows, encryption will be done after installation. This method is also applicable to Linux. We recommend VeraCrypt. Here is a beginner's guide: https://veracrypt.io/en/Beginner%27s%20Tutorial.html.

Passwords

A good password consists of random words/characters, including lowercase letters, uppercase letters, symbols and numbers. Ideally, aim for a minimum of 15 characters.
Password manager: A password manager can generate strong passwords and remember your passwords. The practical advantage is that you only have to remember one password, the one that allows you to access your manager. The downside is that if this password is cracked by someone, they will then have access to all of your stored passwords. Good managers include Keepassxc and Bitwarden. It is best not to use the native manager (provided by your machine by default).

3. DOCUMENTS AND CLOUDS

Create a shared drive on https://cryptpad.fr/. Simply log in to access the drive.

This drive must be TOP SECRET. Do not send it to just anyone, only to trusted individuals connected to the organisation. Do not put just anything on it either.

Regularly clean up this drive so that you do not leave compromising files lying around that are no longer needed.

It is good practice to change the password to access the drive regularly. This password must be given securely and only to trusted individuals who need access to the drive.

- Always access the drive using a VPN+TOR.
- Never access the drive on your phone!
- Warning: if you want to share a cryptpad or a file, you must click on share and not copy and paste the URL of the page.
- Optional: it is possible to schedule the destruction of a cryptpad or files. If destruction is not scheduled: delete the pad after the action, or when it is no longer needed.
- Do not put your name/location/date/personal information on the pad.

4. SIGNAL

Signal, with its end-to-end encryption, is a very good messaging app. But if the police get hold of your phone, they will be able to access your conversations and your friends' profiles. As each profile is linked to a phone number and therefore to an identity card, the whole group will then be identified. Here are a few tips to avoid this:

On an individual level
Enable screen lock for Signal:
- In your account: Settings > Privacy > Screen lock > 'Enable screen lock'
- Set the lock time to a few minutes.
- It is therefore important to have a strong PIN or password on your phone, as Signal uses the same PIN. The longer and more random the password, the better.

Hide your phone number:
- In your account: Settings > Privacy > Phone number > 'Who can see my phone number' > Nobody
- Settings > Privacy > Phone number > 'Who can find me using my phone number' > Nobody

Disappearing messages:
- Enable disappearing messages by default, so that they apply to any new conversations you start: Settings > Privacy > Disappearing messages > Choose the duration of your choice.
- Messages in these conversations will be deleted after this period. The shorter the duration, the higher the security, but the more restrictive it may be.
- You can change disappearing messages in an existing conversation at any time by following these steps. In the conversation: top right > conversation settings > disappearing messages > choose the duration of your choice.
- Please note that this change is not retroactive; messages sent before the change will retain their initial lifetime.

In general

Create a new group every 6 months and only give the link in person or via known and safe contacts. Leave and delete the old group.

Do not discuss private actions/subgroups in a more general group unless necessary.

Before adding someone on Signal, make sure they have basic security knowledge, for example by reading this manual.

Check the list of group members from time to time and if a username doesn't ring a bell, ask your comrades who it is. If no one knows, or if the person has been inactive for a long time, remove them from the group, explaining that they can always contact you if they want to get involved again.

After or just before the action, leave and delete the group.

5. EMAIL

Secure email addresses:
- Protonmail (https://proton.me/mail)
- Riseup (https://riseup.net/en/email/settings/mail-accounts)
- Other emails: systemli.org ; autistici.org ; immerda.ch

Please note that exchanges are only automatically encrypted between the same hosts (i.e. from one Proton address to another Proton address, for example). To encrypt an email between two different providers, you need a public encryption key/open PGP (= asymmetric encryption):

PGP with Protonmail
With Protonmail addresses, it is easy to generate a public encryption key to share with your correspondent.

On Proton: new message > ... (at the bottom) > attach a public key (more info https://proton.me/support/how-to-use-pgp)

It is less easy for your correspondent to integrate it into their email if they do not have one of the addresses mentioned above.

VPN
A VPN (Virtual Private Network) is a service that creates a secure, encrypted connection between your device and the Internet. In practical terms, it routes your data through an intermediary server, which masks your real IP address and protects your online activity. Thanks to encryption, the information you send and receive becomes unreadable to third parties.

Free and reliable: Proton VPN https://protonvpn.com/ or riseup VPN https://riseup.net/en/vpn.

Paid and reliable: Mullvad https://mullvad.net/en
Avoid using other VPNs, such as Nord VPN, which are not secure or, worse, pose a significant risk of data collection. A VPN is not enough to conduct secure searches, therefore you need to also work with TOR.

6. TOR

The Onion Router, or TOR, refers to an internet network, an encryption protocol and an internet browser. Generally speaking, when we talk about TOR, we are referring to the internet browser. This browser routes search data through the TOR network and applies its encryption protocol to protect it.

Because of all these measures, the connection can be slow or even interrupted at times, some sites may not display properly, and others may decide to block connections via TOR.
You can find more information on the TOR project website: https://support.torproject.org/about-tor/.

Downloading and installing the TOR browser is very simple. Just go to: https://www.torproject.org/download/. There are also other browsers that integrate Tor, such as Brave or Mullvad.

Please note: TOR is not all-powerful; it only makes it more difficult to track or identify you online. Using TOR should not make you forget basic security practices.

7. ACTION PHONES

If you need to take a phone with you in action, for instance to take photo's and video's, make sure this phone is not linked to your identity:

- Buy a 'clean' phone, this can be a second hand one, but not an old phone you or your friends or family members have used before. Go to a phone shop and pay cash.
- Use an anonymous sim-card. For this you will need to go to the Netherlands.

For the Dutch SIM-card, make sure you activate the SIM card and mobile internet in the Netherlands in a 'clean' phone. Only then will the phone work in Belgium. Make sure you buy extra call credit in the Netherlands, as the credit you can buy in Belgium does not work with Dutch SIM cards. Lebara works best. Pay everything with cash.

Never turn on this burner phone in your home or any other place linked to you, and do not connect it to the Wi-Fi at home or at work without a VPN. Also, if you go outside to use it, leave you own phone at home or put it in advance on flight mode. Don't use a phone that you have used for other actions already.