**Operations**

**MEETINGS**

*BASIC*

**1. Why Meetings?**

For many people activists, journalists or aid workers, meetings can be high-risk encounters. Meetings can expose the identity or work of either you or the person you meet with, and have often been the scene of arrests. For this reason, it is vital to put the highest level of planning and preparation into meetings involving vulnerable human rights defenders or whistleblowers.

**2. Location Selection**

You should choose the area you plan to meet in carefully. It should be an area the person you are meeting (and you if possible) is comfortable in and knows well. If you don’t know it – get to know it. You should be able to plan out your approach, possible escape and nearby safe spots such as partners, supportive local population, and embassies.

Once you have chosen the area, you need to choose the specific meeting location. Often the most obvious locations such as their office/home offer a false sense of security and you can be more likely to be under surveillance there. It may be better to meet in a public place such as a café. In choosing a café, be careful of the usual spots that human rights defenders frequent – Perhaps adversaries are aware of this this too. Try to choose a location not frequented by people likely to be targeted by surveillance. If you don’t know a location and will not get a chance to see it before you arrive, use the internet to try and view pictures and gather information about it.

Think about various aspects that may allow you to fit in:

* Who are the clientele who use it?
* What do they wear?
* What size groups do they sit in?
* Are the tables so close to each other that you can be easily overheard?
* Is it likely to be crowded?
* Would you look suspicious entering there?

Try to check if there’s there a place to sit where you can observe the whole location but still have your back to a wall and be close to / have a clear path to an escape route. You should always have an alternative backup meeting place nearby and if you feel there is a risk of surveillance or problems at your first choice location – be ready to switch to it at the very last minute.

**3. Scenarios to Consider**

There are a few scenarios you should play out in your head before you go to your meeting. Some may not put you at any extra risk but it’s useful to have thought them through in advance.

* Will you or they have to travel through checkpoints? If so what is your story?
* What will you do if are delayed?
* What if the person is early /late/ arrives unexpectedly with a third party who you don’t know or trust?
* What is your contact plan for if the person doesn’t show at all?
* What if the person is temporarily insecure – someone else is talking to them, they have been stopped by authorities/ recognised/ are drawing attention to themselves?
* How much information you are going to give the person you are meeting?
* What if they pass you something (documents/USB etc.)? Where will you put it to keep it out of sight?
* What do you expect the person’s reaction to the meeting to be – fear/ anger/ anxiety?
* What will you do if you start to get interest from a third party, whether general or threatening?

**4. Arrival at a Meeting**

If possible you should remove batteries from phones before travelling to the meeting location, so as to avoid remote tracking. (See the **Mobile Phones lesson** for more advice on mitigating the risks of phones)

Ideally all parties would conduct counter-surveillance when travelling to the meeting. See the **Counter-Surveillance lesson** for advice on how to do this. If the person you are meeting is not trained in this, and you are unsure of their security, one of your colleagues may be able to check whether your contact has been followed. You should ensure you are clear before you arrive. If possible you should arrive first and check the area is clear – check the toilets, emergency exits and likely approaches.

Try to sit where you can observe the whole location but still have your back to a wall and be close to/ have a clear path to an escape route. If you have a second colleague available who is not needed in the meeting, they can take a seat nearby with a clear view of you and exits.

Do not commit to staying somewhere by buying something until you are sure you are clear – You might attract suspicion leaving otherwise. Agree a subtle and simple signal to alert your colleague if you feel something is wrong.

**5. The Meeting Itself**

It is important to keep control of the flow of the meeting. After introductions you should begin by mentioning security to the person: agree on your alternate time and place for the meeting if a problem occurs; let them know what you can and cannot do to help them if there is a problem; agree on a discreet signal in case there is a problem.

Avoid ordering meals and pay for what you do get straight away and in cash – This avoids your identification and allows you to make a speedy exit if needed.

Observe people who enter after the person you are meeting, as well as anyone who sits close to you – use knowledge of surveillance teams to assess them. Always trust your instincts – prepare to leave immediately if you feel something is not right.

Avoid incriminating yourself. If possible, avoid writing on paper – you can always ask for details to be sent via encrypted email later. (See the **Email lesson** for advice on how to send encrypted email.) If notes are necessary, try not to write anything sensitive in the first ten minutes and in general keep the amount of sensitive notes you take/actually record to a minimum whenever possible. Consider using codenames (esp. for testimony or sensitive information). When finished with your notes, always remember to destroy them safely and dispose of it in places away from the meeting location. Do not let waitresses or waiters overhear your conversation.

**7. Eavesdropping**

Unfortunately bugging equipment is very cheap, widespread and effective. It is very, very hard to find eavesdropping equipment that has been planted against you – many look like ordinary electronic items. In some countries, many high profile hotels are targets for regular bugging due to the frequent presence of business people, diplomats, NGOs etc.

The best tactic in avoiding such devices is to be unpredictable and change locations frequently if you are on high-risk travel and need to avoid surveillance. Be very wary of conducting sensitive activities in fixed locations (such as the office of a partner or a hotel room) for too long or repetitively. Limiting the provision of information in advance (for example, of which rooms will be used for conferences in specific hotels) is also useful as it reduces the time a hostile organisation has to plant a device. Outside in the open air can also be a good place to discuss sensitive matters. Make sure you are not overlooked.

If dealing with sensitive matters, always assume the room is bugged. Ensure that all mobile phones are turned off and batteries removed (as they can be turned on remotely without you knowing and used as a listening device). If possible you should remove batteries from phone before arriving at meeting location. (See the **Mobile Phones lesson** for more advice on avoiding the risks of phones) Masking noises like a loud radio or TV can be useful for reducing overheard conversations, although the most advanced devices can eliminate these extra sounds.

Unplug all unnecessary electronic devices from the electrical sockets. (If possible, turn off the electricity at the mains and check behind all electrical plug and light switch sockets.) Pay particular attention to smoke alarms, lamps, clocks etc. Don’t forget about staff such as cleaners or waiters who may be able to overhear what is going on.

**8. Leaving a Meeting**

It is best to get the person you are meeting to leave first – that way you can check for any third party reactions to see if they’re clean as they leave. Wait about ten minutes before you leave. If possible your colleague (who should still look unconnected to you) should remain behind for a further ten minutes to check that you are clean.

**9. What now?**

**Swipe right for this lesson’s checklist**

*RELATED LESSONS/TOOLS*

* *Counter-Surveillance lesson*
* *Mobile phones lesson*
* *Email lesson*

***Meetings Basic Checklist***

* ***Meet in an area one of you is comfortable with***
* ***Avoid partner offices/homes/hotels or spots frequented by human rights defenders***
* ***Research the meeting spot***
* ***Think through what you’d do in various scenarios***
* ***Remove batteries from mobile phones before you leave***
* ***Arrive early and conduct counter-surveillance on your way***
* ***Have a colleague observe from afar***
* ***Sit with back to wall, good observation of the location, and clear path to escape route***
* ***Observe others who enter***
* ***Agree security precautions with person you meet***
* ***Avoid ordering big meals and pay straight away in cash***
* ***Trust your instincts and leave immediately if you feel something’s not right***
* ***Avoid writing sensitive notes on paper***
* ***Do not let staff/ waiters over hear you***
* ***Be unpredictable***
* ***If in private room – unplug unnecessary devices and use masking sounds***
* ***Leave last so that you can observe any third party reactions***

**COUNTER-SURVEILLANCE**

*BASIC*

**1. Surveillance**

Surveillance is the monitoring of people’s behaviour, activities, or other patterns for the purpose of harming, influencing, managing, directing, or protecting them.

**Why might people be interested in keeping you under physical surveillance?**

* Break-in/ theft of sensitive materials
* Arrest
* Monitor who is coming and going from the office
* Intimidation
* Physical attack on staff

**Who might be interested in keeping you under surveillance?**

* Authorities of the country in which the regional office is located (police, intelligence, military)
* External security agencies of other countries in the region
* Criminals
* Terrorists
* Private contractors
* Embassy officials of ‘friendly’ countries
* Individuals (may be disgruntled with the organisation)

**2. Surveillance techniques**

**What techniques are available to carry out surveillance?**

* Digital surveillance (monitoring of digital communications, mobile phones etc.)
* Human surveillance (on foot, in a vehicle)
* Technical surveillance (bugs, listening devices, video cameras, number plate readers etc.)

These lessons deal with how to counter human surveillance. For advice on digital surveillance see the **Information** and **Communications** lessons. For advice on how technical surveillance see the **Meetings lesson** and **Home/Office** section.

**3. Identifying office surveillance**

**How to Identify if Your Office is Under Surveillance**

Surveillance generally requires that the adversary is able to observe the activities of its targets. This means there are a limited number of physical sites they can use for surveillance. The best thing to do when looking for surveillance is to try to think like an adversary – what might you do is you were trying to monitor your office? From where might you carry out such surveillance?

* **Take a baseline**
  + It is important to gain an understanding of what “normal” conditions look like. (For example, where cars normally park or people normally stand).
* **Identify and record**
  + From this, try to identify and record any unusual activities. (For example, people in locations where they shouldn’t be or aren’t normally).
* **Filter out coincidence** 
  + Filter out the chances that something could be a coincidence by concentrating on unusual activities and applying common sense filters (e.g. if someone is standing in a place where people don’t normally stand pay more attention to them. Do they look like they are from the area? Are they paying an unusual amount of attention to your activities?) Look for 3 signs that something is out of the ordinary or 3 repeat sightings.
* **Notify others**
  + It is important to notify others of any suspicions and to keep a log of them. This allows the monitoring of patterns which otherwise might not emerge. For example, if you notice someone suspicious and then a colleague notices something else suspicious on a separate occasion but this information is not shared, then a valuable opportunity to confirm a security threat is missed.
* **Trust your senses**
  + Trust your senses – there may be clues of a potential arrest or violent attack. Often, HRDs report that there were warning signs prior to an attack, but they chose to ignore the warning signs or dismissed it as paranoia.

**4. What to do**

**What To Do If Your Office Is Under Surveillance**

* **Consider the risks**
  + Confrontation with suspicious people should be done with caution, before doing so, consider the risks. For example, what might that person be doing? What is the past history of threats against your organisation or yourself? Is it likely that they will attack you immediately if you confront them or is it more likely that they will just leave and send someone else? If you confront someone they are likely to be replaced by another (unknown) agent, and you then lose the benefit of being able to monitor the surveillance being carried out against you.
* **Increase protection**
  + Increase your office protection by reducing the ability of an adversary to conduct surveillance. For example by putting up screening near your building, using CCTV and/or guards, closing blinds, locking gates, selecting sites which are not easily overlooked, strict access controls to your building etc.
* **Continue monitoring**
  + Continue to monitor the general security environment and increase your observation of threats during periods of higher tension – e.g. protests, elections, sensitive national holidays etc.

**5. What now?**

**Swipe right for this lesson’s checklist**

**Go to the Advanced Lesson for advice on how to practice counter-surveillance when you are out on foot.**

**Go to the Expert Lesson for advice on how to practice counter-surveillance when you are out in a vehicle.**

*RELATED LESSONS/TOOLS*

* *Malware lesson*
* *Passwords lesson*
* *Protecting Files lesson*
* *Making a Call lesson*
* *Sending a Message lesson*
* *Email lesson*
* *Radio lesson*

***Counter-Surveillance Beginner Checklist***

***To identify surveillance of your office***

* ***Take a baseline***
* ***Identify and record unusual activity***
* ***Filter out coincidence***
* ***Notify others***
* ***Trust your senses***

***If under surveillance***

* ***Consider risks of confrontation***
* ***Reduce the ability to watch you***
* ***Increase protection***
* ***Continue monitoring***

*ADVANCED*

**1. Countering Surveillance on Foot**

Physical surveillance continues to be a significant danger to those working on human rights. Other than a human source, it is the only way to build detail on what is occurring at meetings. It is obviously important to know how to identify if you, your colleagues, or partners are under surveillance.

*Counter-surveillance* is the process of detecting and mitigating hostile surveillance. This lesson lets you know how to practice counter-surveillance at one of the most important times – when you are out and about on foot, such as going to a sensitive meeting.

For advice on how to practice counter-surveillance when in a vehicle, go to the Expert lesson.

**2. WHAT DO THEY LOOK LIKE?**

There are a number of indicators that might let you know if a person is conducting surveillance on foot.

Look out for:

* Bulky, loose clothing
* Outdoor clothing
* Military-style sports watch
* Radio broadcast switch on their wrist
* Earpiece with/without a wire
* Comfortable footwear

Surveillance teams often try to use people who would easily be overlooked. Don’t disregard people such as:

* Females
* Couples/groups
* People wearing expensive clothes
* Young/old looking people
* People jogging
* Beggars
* Hotel maids, gardeners
* Road workers
* Commercial outfits (e.g. electricity company)
* Unlikely minorities
* People with a pram/dog/shopping bags

‘Tells’ that might give away someone who is conducting surveillance on foot include:

* Readjusting personal equipment
* Touching earpiece
* Visibly talking into their microphones
* Glazed eyes
* Unusual behaviour or demeanour
* Trying to avoid the target’s gaze
* Looking around corners/through windows
* Mirroring behaviour
* Stopping in unusual places

**Identifying Teams**

If you identify one potential surveillance member, you can use that knowledge to identify others. Members of a surveillance team can cross-contaminate other members:

* By speaking directly to them
* By looking in their direction
* By using hand signals
* By appearing or dressing in a similar manner

**3. WHAT CAN YOU DO TO SPOT THEM?**

The most important thing to remember when conducting counter-surveillance is that you need to be discreet – you do not want any potential surveillance teams to know that you are looking for them. This would raise suspicions further about what you intended to do. **The primary aim is to ascertain whether or not you are being followed, not to lose them.**

Remember, if you discover you are in fact under surveillance, you have three options:

* **Change your plans**: This is the safest and recommended option – it will allow you to keep your original plans to yourself and reassure whoever had you under surveillance that you aren’t up to anything suspicious or worthy of surveillance.
* **Lose the surveillance covertly**: This is losing the surveillance team without them knowing you were aware of them by making it look accidental. This should be used if you absolutely must keep your plans and you feel it is safe to do so.
* **Lose the surveillance overtly**: This trying to identify or lose the surveillance team in a way that makes them aware of what you are trying to do. This is a risky tactic because it confirms to the team that you are indenting to do something that you don’t want them to see and so are increases the likelihood of you being under continued surveillance. You should only conduct your counter-surveillance overtly if absolutely vital and it is not possible to do so covertly.

**4. Five Rules of Counter-Surveillance**

1. **Trigger**
   * This is the person who initially alerts the rest of the surveillance team when the target is on the move. The easiest person to find.
2. **10 to 2** 
   * The person carrying out the surveillance will try to stay *out* of a the 10 t0 2: the immediate eye line of the person they have put under surveillance
3. **3 times** 
   * This is the number of sightings of a surveillance team member you are aiming to achieve before you can confirm that you are under surveillance.
4. **3 sides of a square**
   * This is the minimum number of turns you take to filter and reduce the possibility of seeing the same person by coincidence.
5. **Breaking the box** 
   * This is the process of breaking out of the surveillance a team will try to keep you in. By breaking the box you increase the likelihood that they will make mistakes which you can observe and use to identify them.

* **5. Tactics: Identify the Trigger**

The trigger is the surveillance team member who initially alerts the rest of the surveillance team members (who will be spread out in a box around the target). They are unlikely to move when you leave your location as that may draw attention to themselves.

The easiest place for them to be located is in or outside your location. They will usually try to stay stationary. If the place you have entered has a number of exits then a number of team members may be spread around each as a trigger. Think about where you would be if you were on a surveillance team – look for locations and situations where it would not be suspicious for a surveillance person to be hanging around.

* **6. Tactics: How to find the eyeball on foot**

The eyeball refers to the member of the surveillance team who currently has you in their sights. Firstly - *don’t look over your shoulder!* Instead try to create situations to look observe all around you naturally – including behind you:

* Try using windows – either looking through them or in their reflection – or car mirrors;
* Hold open doors for other people to enter and let them overtake you;
* Cross a busy street and see who follows you;
* Stop to look at posters or bus timetables, use an ATM, or buy something from a street vendor.

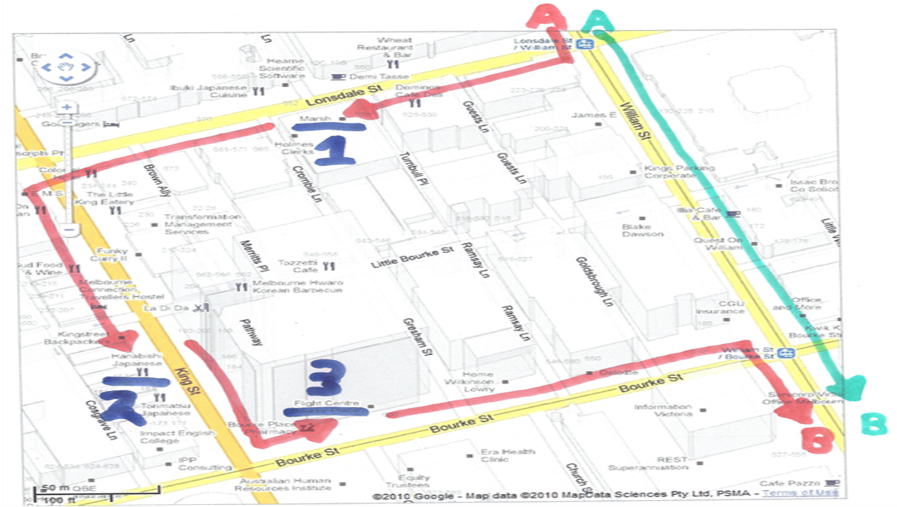
* **7. Tactics: Create a force-past**

A force-past is when you create a situation in which someone following you would have to go past you or expose their position. There are several easily created force-past points:

* Traffic crossing point
* Bus stop
* Taking an escalator
* Using a lift to go up (until all passengers have left), then go down and exiting via an underground car park
* Rapidly turning a corner then suddenly entering into a shop
* Go into a shop/pub/building through one entrance and then rapidly exit via another
* Corner hanging – turn a corner then rapidly stop
* Change your clothing to make it harder to identify you
* **8. Tactics: Three Sides to a Square**

This is a technique used to identify several members of a team, create pressure on them and thin down their surveillance. It can be conducted alone or with a team.

It means taking a longer route than would logically make sense for someone going from point A to B.



Pick three or more reasons to be a) using such an unusual route and b) stopping along the way. These reasons should take the following things into account:

* It should be genuine and not suspicious – there should be a believable reason for the detour. Remember, this is because you do not want any possible surveillance to know that you are checking for surveillance;
* It should force a surveillance team member to go into the location with you to establish what you are doing, who you are meeting, or check for any signs that you may have a counter-surveillance team with you;
* It should be a position where you can:
  + Observe what is occurring
  + Observe the various exits/entrances
  + Be out of the target’s 10 to 2 eye line
* You should be able to quickly get on the move again – so pay bills in advance, don’t get hot food, etc.
* **9. Tactics: Get on a bus**

It is difficult for surveillance teams to keep up if you suddenly get on a bus, going from on foot to mobile. This is particularly true because buses are slower than other vehicles so are difficult to follow by car too. Ensure you have change for the fare. Sit as far back in the bus as possible and if it’s left-hand drive, sit on the right side of the bus to be able to observe any vehicles which might over take the bus

If conducting *overt* anti-surveillance – get on, get off at the next stop, and then rapidly get on the next bus. If you want to appear *covert* – get on a bus with one number, then get off and get a bus with another number, to make it look like you might be lost.

* **10. Tactics: Get in a train or taxi**

Trains are difficult to follow with multiple forms of surveillance because they are faster than other vehicles. When getting on the train, hang back and try to be the last person to get on. Stand at the end of the platform where the train driver stops and where you will have a good view. Try buying a ticket to a destination and observe - get off before that destination.

If conducting *overt* anti-surveillance – get off then rapidly change trains. If you want to appear *covert* – get on a train with one destination, then get off and get a train with another destination, to make it look like you might be lost.

Taxis can be useful for local knowledge and the fact that in some countries they can use bus lanes which surveillance vehicles might not be able to use without drawing attention to themselves.

**9. What now?**

**Swipe right for this lesson’s checklist**

**Go to the Beginner Lesson for advice on how to identify and deal with surveillance of your office.**

**Go to the Expert Lesson for advice on how to practice counter-surveillance when you are out in a vehicle.**

*RELATED LESSONS/TOOLS*

* *Meetings*

***Counter-Surveillance Advanced Checklist***

***To identify on foot surveillance***

* ***Look for typical comfortable clothing and accessories***
* ***Don’t overlook atypical people***
* ***Look for behavioural tells that they’re concentrating or communicating***

***Actions to help you spot them***

* ***Be discreet***
* ***Look for 3 sightings***
* ***If being followed you should change plans***
* ***Identify the trigger***
* ***Create situations to find the eyeball***
* ***Create a force-past***
* ***Make 3 sides of a square***
* ***Get on a bus/train/taxi***

*EXPERT*

**1. Countering Surveillance in a Vehicle**

Physical surveillance continues to be a significant danger to those working on human rights. Other than a human source, it is the only way to build detail on what is occurring at meetings. It is obviously important to know how to identify if you, your colleagues, or partners are under surveillance.

*Counter-surveillance* is the process of detecting and mitigating hostile surveillance. This lesson lets you know how to practice counter-surveillance at one of the most important times – when you are in a vehicle, such as going to a sensitive meeting.

For advice on how to practice counter-surveillance when on foot, go to the Advanced lesson.

**2. WHAT DO THEY LOOK LIKE?**

There are a number of indicators that might let you know if a vehicle is being used to conduct mobile surveillance.

Look out for:

* Common vehicles for the area – a team will try to use the most inconspicuous vehicle for the local environment
* Unusual aerials
* Modified boxes on top
* Equipment in the car – Maps, radios, GPS, binoculars, cameras etc.
* Rubbish in a car
* Parking for quick exit
* Windows left slightly open
* “Boot fit”
* One or at most two people in a vehicle
* Radio operator talking into a radio
* Two people in a stopped car talking but not apparently to each other
* Leaving an engine on unnecessarily
* Brake lights being activated when a vehicle is stationary
* Don’t forget taxis, rickshaws or expensive looking cars.

**Identifying Teams**

If you identify one potential surveillance member, you can use that knowledge to identify others. Members of a surveillance team can cross-contaminate other members:

* By looking in their direction
* By using hand signals
* By parking their car or stopping in the same place (e.g. they have relieved each other)
* By poor discipline/drills/boredom and pulling their cars up alongside each other in order to have an unnecessary conversation.

**3. WHAT CAN YOU DO TO SPOT THEM?**

The most important thing to remember when conducting counter-surveillance is that you need to be discreet – you do not want any potential surveillance teams to know that you are looking for them. This would raise suspicions further about what you intended to do. **The primary aim is to ascertain whether or not you are being followed, not to lose them.**

Remember, if you discover you are in fact under surveillance, you have three options:

* **Change your plans**: This is the safest and recommended option – it will allow you to keep your original plans to yourself and reassure whoever had you under surveillance that you aren’t up to anything suspicious or worthy of surveillance.
* **Lose the surveillance covertly**: This is losing the surveillance team without them knowing you were aware of them by making it look accidental. This should be used if you absolutely must keep your plans and you feel it is safe to do so.
* **Lose the surveillance overtly**: This trying to identify or lose the surveillance team in a way that makes them aware of what you are trying to do. This is a risky tactic because it confirms to the team that you are indenting to do something that you don’t want them to see and so are increases the likelihood of you being under continued surveillance. You should only conduct your counter-surveillance overtly if absolutely vital and it is not possible to do so covertly.

**4. Five Rules of Counter-Surveillance**

1. **Trigger**
   * This is the person who initially alerts the rest of the surveillance team when the target is on the move. The easiest person to find.
2. **10 to 2** 
   * The person carrying out the surveillance will try to stay *out* of a the 10 t0 2: the immediate eye line of the person they have put under surveillance
3. **3 times** 
   * This is the number of sightings of a surveillance team member you are aiming to achieve before you can confirm that you are under surveillance.
4. **3 sides of a square**
   * This is the minimum number of turns you take to filter and reduce the possibility of seeing the same person by coincidence.
5. **Breaking the box** 
   * This is the process of breaking out of the surveillance a team will try to keep you in. By breaking the box you increase the likelihood that they will make mistakes which you can observe and use to identify them.

* **5. Tactics: How to find the eyeball**

When looking for repeat sightings in a vehicle, use the following tactics if safe to do so:

* Look for repeat sightings
* Use a false indicator
* Drive fast / slow
* Stop suddenly (try to have a reason for this – such as pulling in at a petrol station at the very last minute or taking a mobile phone call)
* U-turn
* Move into a filter lane turning right and at the last minute continue straight
* Stop immediately after taking a left turn – will force others to overtake
* Change lanes
* Turn into a dead end
* Enter onto a fast road such as a dual carriageway/motorway and then come off it quickly
* Exit a dual carriageway/motorway and then come straight back onto it again
* Use your mirrors
* Create opportunities to look around
* Stretch out the team
* Create opportunities (if absolutely vital) to evade a surveillance team

If the political environment allows, pull in to a police station or ring colleagues/ backup to meet you at a designated spot where you can aim to safely lead any potential surveillance team members which you haven’t broken contact with.

* **6. Tactics: Chokepoints**

Chokepoints are areas that anyone following you must pass through, and so allow for better observation and filtering of potential surveillance. Some naturally occurring chokepoints could be:

* Small relatively deserted laneway/alleyway with few paralleling lanes/roads
* Traffic lights
* Roundabouts
* Road junctions
* One way streets
* Car park entrances/exits
* Toll booths
* Quiet roads
* Long straight roads
* Road works

If using a roundabout as a chokepoint, try to record up to 10 of the vehicles following the vehicle which is potentially under surveillance – Try to note the registration and description (colour, make, model, unique descriptive features, number of occupants, presence of radios etc.) This is because a handover to another car may take place here – so another person would now have the target in their line of sight.

Look for a handover: When turning, look for vehicles (or people on foot) who might match the profile of surveillance team members but then continue straight.

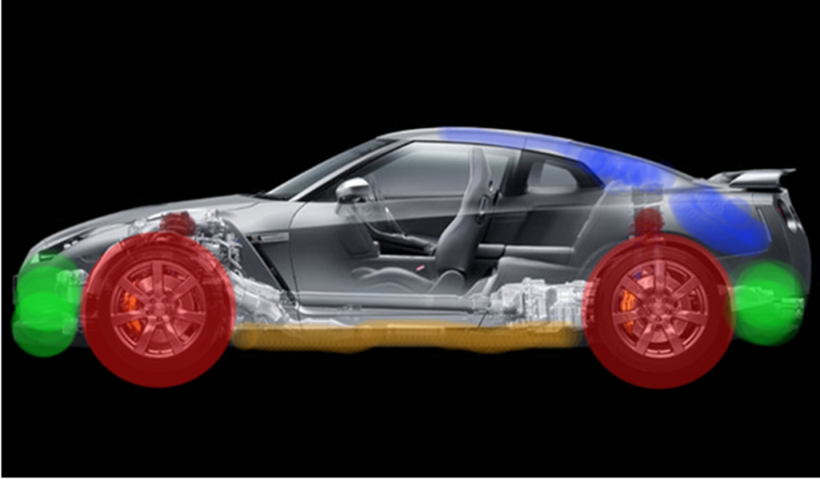
* **7. Spotting Trackers**

A tracker is a device placed on a car to monitor its location. This is often used by surveillance teams instead of physically following a person’s car.

Some trackers (particularly those used by government agencies) allow the surveillance team to track a target in real time and to monitor historical paths. Some trackers only log the journey taken by the target vehicle. They do not allow the surveillance team to track the vehicle live – instead the tracker must be retrieved by the team and analysed on a laptop.

You should be particularly aware of the risk of trackers if you think your work is of interest to the authorities and your car is kept in a publicly accessible areas at any time. You should regularly check your car for trackers and particularly before going to any sensitive meetings.

Trackers are usually placed on the base of a car using magnets. They can also be placed in the boot or roof. You need to get right under the car and feel around corners with your hands to do a proper check.



Trackers can be the size of a phone or even smaller. They can also be covered in tape or oil to help disguise it as part of the car.



**8. What now?**

**Swipe right for this lesson’s checklist**

**Go to the Beginner Lesson for advice on how to identify and deal with surveillance of your office.**

**Go to the Advanced Lesson for advice on how to practice counter-surveillance when you are out on foot.**

*RELATED LESSONS/TOOLS*

* *Meetings lesson*
* *Mobile phones lesson*

***Counter-Surveillance Advanced Checklist***

***To identify mobile surveillance***

* ***Be aware of the most common types of vehicle***
* ***Don’t overlook taxis or service vehicles***
* ***Look for aerials or modifications***
* ***Look for signs of people being in the car for long periods of time***
* ***Look for signs of people communicating covertly***

***Actions to help you spot them***

* ***Be discreet***
* ***Look for 3 sightings***
* ***If being followed you should change plans***
* ***Create situations to stop***
* ***Use your mirrors***
* ***Use chokepoints***
* ***Monitor several cars back***
* ***Check for trackers***

**PROTESTS**

*BASIC*

**1. Before You Go**

Protest marches, rallies or unplanned gatherings may be small and self-limiting or may become riots and civil disturbance.

It is important to prepare adequately (in proportion to the expected event) before going to cover it. This can have many different meanings depending on the size of the team you work with, but should include the following if possible and appropriate:

* Prepare emergency and fall back plans – agree at what stage you should pull out and emergency meeting points;
* Source and pack protective equipment – see the **Protective Equipment lesson** for more advice on this;
* Pack a first aid pack – you should also remind yourself of how to administer basic first aid;
* Select broadcast equipment carefully – you may want to use discreet cameras if filming becomes dangerous;
* Contact your Safety Adviser or the person responsible for security in the organisation you are contracted to – they should consider the size of team needed and whether or not it should include security personnel;
* Teams covering disorder, riots etc should have training and briefing on safety in civil unrest situations. Experience is also a great help.
* For large protests a specific risk assessment should be carried out.

**2. Dealing with Crushes**

Crushing in crowds or police charges can be dangerous even as a bystander. You can mitigate the danger by taking the following precautions:

* Ensure there are good working communication channels between the team and everybody’s location is known at all times.
* Unless specifically planned to cover from amongst crowd, retreat to a safe vantage point, e.g. an upstairs window of a nearby building with permission of the owner.
* Park vehicles in accessible location, positioned for easy departure. Plan positions including emergency escape routes & fallback plans.
* Take second person and stay alert to changes in situation – leave if crowd behaviour becomes unpredictable.
* Wear clothing & footwear that will enable easy movement around any debris. Do not wear high heels or sandals / open toed shoes.

**3. Dealing with Violence**

Violence in a crowd situation can include physical harassment, thrown debris, petrol bombs, fire, use of weapons or tear gas. To mitigate such dangers, you should take all the precautions outlined under “Dealing with Crushes” as well as the following:

* Wear suitable protective clothing e.g. fire retardant natural fibres.
* Trust your instincts – crowds can turn very quickly. If you sense it is becoming unsafe or you are getting too much attention, withdraw to a safe area.
* If faced with direct aggression / if weapons appear, withdraw to a safe area immediately and tell your team.
* Take riot kits if appropriate. Riot kits containing equipment (safety glasses, bump cap, mask etc) and first aid kits are made available by large media organisations.

**4. What now?**

**Swipe right for this lesson’s checklist**

**Go to the Advanced lesson for advice on partaking in protests as an activist.**

*RELATED LESSONS/TOOLS*

* *Protective Equipment lesson*

*FURTHER READING*

* [*BBC Journalism Safety Guide*](https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCEQFjAA&url=http%3A%2F%2Fdownloads.bbc.co.uk%2Fmundo%2Fpdf%2Fsafety-journalism_safety_guide_second_edition-v1.pdf&ei=NlNnVePCLobbsATcsYL4Cg&usg=AFQjCNGP2fOBeJm5d3zj_BdsbnbjSMf6MA&sig2=I2v5tLpgbfQrD7bfjPZDNw&bvm=bv.93990622,d.ZGU)

***Protests Basic Checklist***

* ***Prepare emergency plans***
* ***Pack protective equipment***
* ***Pack a first aid kit and remind yourself of the basics***
* ***Select appropriate broadcast equipment***
* ***Talk to your Safety Adviser if possible***
* ***Get training in dealing with civil unrest***
* ***Conduct risk assessment***
* ***Ensure working communications***
* ***Cover from safe vantage point if possible***
* ***Park vehicles in accessible location for easy departure***
* ***Take second person into crowd to monitor changes***
* ***Wear appropriate clothing and footwear***
* ***Trust your instincts***
* ***Withdraw if faced with aggression***
* ***Take riot kits***

*ADVANCED*

**1. Should You Bring Your Phone?**

Activists and human rights defenders are increasingly documenting their protests using cameras and mobile phones – often to powerful effect. The following are useful tips for you to remember if you are going to a protest and are concerned about protecting your electronic devices if you’re detained by police.

Think carefully about what’s on your phone before bringing it to a protest. Your phone contains a wealth of private data, which can include your list of contacts, the people you have recently called, your text messages and email, photos and video, GPS location data, your web browsing history and passwords, and the contents of your social media accounts. Through stored passwords or active logins, access to the device can allow someone to obtain yet even more information on remote servers. (You can log out of these services).

In many countries, people are required to register their SIM cards when they purchase a mobile phone. If you take your mobile phone with you to a protest, it makes it easy for the government to figure out that you are there. If you need to keep your participation in a protest secret from governments or law enforcement, cover your face so that it is harder to identify you from photos. However, do note that masks may get you into trouble in some locations due to anti-mask laws.

**If it is important to keep your presence at the protest concealed, *do not take your mobile phone with you.***

**If you absolutely must bring a mobile phone with you, try to bring one that is not registered in your name.**

**2. Preparing Your Phone**

To protect your rights, you may want to harden your existing phone against searches. For the full set of advice on how to manage the security of your mobile phone, go the **Mobile Phone Lesson**.

* **Passwords**: Always password-protect your phone. While password-protecting your phone is a small barrier to access, please be aware that it is *not* an effective barrier to expert forensic analysis.
* **Encryption**: Some phones have encryption options available – these should be applied. If you have an Android phone this can be done in *Settings -> Personal -> Security -> Encryption*. The Electronic Frontier Foundation has a guide on how to encrypt [i](https://ssd.eff.org/en/module/how-encrypt-your-iphone" \l "overlay=en/node/48/" \t "_blank)**[Phone](https://ssd.eff.org/en/module/how-encrypt-your-iphone" \l "overlay=en/node/48/" \t "_blank)**s.
* **Download secure apps:** Make sure you and your colleagues have downloaded apps that will allow you to communicate and operate securely. (These are explained in detail later in this lesson)
  + **For communicating**: [Textsecure](https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms&hl=en_GB) and [RedPhone](https://play.google.com/store/apps/details?id=org.thoughtcrime.redphone&hl=en_GB) (for Androids) or [Signal](https://itunes.apple.com/gb/app/signal-private-messenger/id874139669?mt=8) (for iPhones)
  + **For filming/photographing**: [ObscuraCam](https://guardianproject.info/apps/obscuracam/) and [InformaCam](https://guardianproject.info/2012/01/20/introducing-informacam/%5D" \t "_blank)
  + **For emergencies**: [**Panic Button**](https://panicbutton.io/#home) (Android only)
* **Back up your data:** It’s important that you frequently back up the data stored on your phone, especially if your device lands into the hands of a police officer. You may not get your phone back for a while (if at all) and it is possible that its contents may be deleted, whether intentionally or not.
* **Keep an emergency number:** Consider writing one important, but non-incriminating phone number on your body with a permanent marker in case you lose your phone, or are in police custody but are permitted to make a call.
* **Use a throwaway**: You should also consider bringing a throwaway or alternate phone to the protest that does not contain sensitive data, which you’ve never used to log in to your communications or social media accounts, and which you would not mind losing or parting with for a while. If you have a lot of sensitive or personal information on your phone, or you need to conceal your presence at the protest, this might be the best option for you.

**3. Plan Ahead**

If you are concerned about being arrested at the protest, it’s best practice to pre-arrange a message to a trusted friend or colleague who is in a safe place. Write your text message to that person in advance and queue it up so that you can send it quickly in case of an emergency to let them know you have been arrested.

If you have an Android phone an easier way of doing this is by using an app, [**Panic Button**](https://panicbutton.io/#home), which turns your mobile phone into a secret alarm for when you're in trouble. When triggered, it sends alerts every 5 minutes with your location to your chosen contacts. This is a very useful tool to have when going to a protest where trouble could occur and we recommend you download it before you go.

Similarly, you may want to plan a pre-arranged call after the protest with a friend—if they don’t hear from you, they can assume you’ve been arrested.

In addition to being made aware that your phone has been seized and you have been arrested, that trusted friend might be able to change the passwords to your email and social media accounts in case you are coerced into giving up your passwords to the authorities.

**4. Understand the Risk**

Please note that deliberately concealing or destroying evidence may be considered an illegal act in itself in some jurisdictions (including many social democracies).

Be sure you understand the law and the risks before engaging in this plan. For instance, if you are protesting in a country with a strong tradition of the rule of law and where protesting in itself is not a crime, it may be that conspiring to lock out law enforcement from your accounts may lead to you breaking the law when previously you would be able to leave without charge.

On the other hand, if you are concerned for the physical safety of you and your colleagues at the hands of a unchecked militia, protecting your contacts’ identities and your own data from them may be a greater priority than complying with an investigation.

**5. At the Protest**

Once you are at the protest, keep in mind that law enforcement may be monitoring communications in the area. You may wish to encrypt your messages using [Textsecure](https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms&hl=en_GB) (Androids) or [Signal](https://itunes.apple.com/gb/app/signal-private-messenger/id874139669?mt=8) (iPhones), or encrypt your phone calls using [RedPhone](https://play.google.com/store/apps/details?id=org.thoughtcrime.redphone&hl=en_GB) (Androids) or, again, [Signal](https://itunes.apple.com/gb/app/signal-private-messenger/id874139669?mt=8) (iPhones). All these apps are compatible. You can read more about them in the **Sending a Message** or **Making a Call** lessons.

Please remember that even if your communications are encrypted, your metadata is not; this means your mobile phone will still give away your location and information such as whom you are talking to and for how long.

When capturing pictures or video it is important to be careful of privacy and safety of those pictured. For example, if you take photos or record video of a sensitive event, it might be dangerous to you or to those who appear in the recordings if your phone fell into the wrong hands. The Guardian Project has created an app called **ObscuraCam** to detect/select faces on photos and blur them. It also deletes the original photos and if you have set up a server to upload the captured media, it provides an easy way to upload it.

Metadata such as phone identity and location are also captured on photos and videos. In some instances, such information is really important to have to prove the credibility of images and video so that they could be used as evidence in courts of law. At other times metadata can put you or others at risk. The GuardianProject has made a plugin tool for ObscuraCam called [InformaCam](https://guardianproject.info/2012/01/20/introducing-informacam/%5D" \t "_blank) that allows you to store a version of the image/video with metadata while also creating a redacted version without any sensitive data that can safely be shared on social media.

**6. What now?**

**Swipe right for this lesson’s checklist**

**Go to the Beginner lesson for advice on covering a protest as a journalist.**

*RELATED LESSONS/TOOLS*

* *Mobile Phone Lesson*
* *Sending a Message Lesson*
* *Making a Call Lesson*

*FURTHER READING*

* [*EFF – Attending protests*](https://ssd.eff.org/en/module/attending-protests-international)

***Protests Advanced Checklist***

* ***Don’t take your phone unless you really need to***
* ***Consider bringing something to hide your face***
* ***Consider bringing a throwaway phone***
* ***Password protect your phone***
* ***Consider encrypting your phone***
* ***Download secure apps in advance***
* ***Back up your data***
* ***Write down an emergency number***
* ***Make an emergency plan with a friend***
* ***Prepare Panic Button app***
* ***Understand legalities and risks***
* ***Use TextSecure and RedPhone, or Signal to communicate***
* ***Use ObscuraCam and InformaCam for photos or videos***

**ARREST**

*BASIC*

**1. Prevention**

Human rights workers, journalists and humanitarian staff are sometimes arrested or detained. The risk of this happening can be significantly reduced by:

* Good relations with local authorities and groups where possible
* Appropriate behaviour, on and off duty
* Obeying local laws and customs
* Ensuring that all legal documentation is correct, and carried by all staff and vehicles as required
* Training and briefing staff before they begin their assignments

Be aware of which areas and groups benefit from aid and which do not, and therefore might feel discriminated against, and make sure that as many people as possible in the area of operations understand your organisation and the role it is playing. Transparency, good communications, integrity, even-handedness and respectful attitudes help as well.

**2. Organisational Response**

* If a staff member is arrested and their whereabouts are unknown, the first priority is to establish where they are and under whose authority. Be assertive and visit all relevant local authorities, inform the embassy (in the case of an international staff member) and be very persistent and insistent in seeking information.
* Remember that a staff member may be arrested for legitimate reasons and may have to account for their actions. Either way, engage a good local lawyer, who knows the local languages and the local system, has experience with this type of situation and perhaps has useful connections.
* When it is clear who has arrested the staff member and where they are, seek to ensure that their rights are protected. Insist on their right to be visited and to medical and legal assistance, and request improvements in the conditions in which they are being kept, if these are not acceptable. Protest if these requests are not met. It is important to find out from them exactly what happened.
* People are often arrested without formal charges being brought, in which case insist that a charge is articulated within a specified period of time. The charge may relate to the individual (for example they are accused of being involved in a crime) or the organisation (for example an accusation of spying under cover of humanitarian work). In any scenario the main priority is to work towards the safe and speedy release of the staff member. In most circumstances, only once a staff member is freed from wrongful charges should efforts be made to clear the name of the individual or the organisation.
* Liaise with, and manage, the staff member’s family. Tell them the steps being taken, maintain a direct regular line of communication, remain aware of what steps the family intends or has taken, and warn them if what they plan to do looks like it may be counter-productive.
* Inform other humanitarian organisations, such as the ICRC, and ask their advice, if appropriate. In many cases, the knowledge that other international organisations are aware of the detention may be enough to persuade the authorities to release the detainee.

**3. What to do if Arrested**

Below are some useful pointers to remember if you are ever arrested. If travelling, your protocol for conduct during questioning should be agreed during the planning of the trip.

* Identify yourself clearly as a representative of your organisation where appropriate.
* The most important consideration is to ensure outside help is aware of what is occurring. The [**Panic Button app**](https://panicbutton.io/) can be helpful in letting your friends or colleagues know you are in trouble with just the press of a button.
* Prepare yourself mentally for what might be coming. It requires patience on your part and the ability to keep calm. You might be threatened, assaulted, cuffed, put in a confined space such as a cell, mistreated, intimidated, sleep/food/water deprived etc. In general highlight these issues immediately to the authorities who made the arrest and also your legal support - and make sure they are noted.
* Even in the environments most hostile to the work of HRDs, authorities generally still seek to have a confession (even if it is false or gotten through force) before they take further action. If you remain calm and don’t give this to them, it makes it much harder for them to make false allegations against you.
* Never sign anything you don’t agree with or in a language you don’t understand.
* Know your legal rights and be persistent in requesting that they you are granted them. E.g. to see a lawyer, speak to the embassy, medical treatment etc.
* Be co-operative, calm and helpful but don’t volunteer information unnecessarily. Think about what information is unimportant, such as the general activities of your organisation, and what is high-risk, such as the sensitive data you were recently passed by a whistle-blower.
* Attempt to understand at an early point
  + Who arrested you?
  + Where are they taking you?
  + What type of organisation is behind it? (Local police might have a very different agenda then a national intelligence agency)
  + Who else was arrested?
  + Why were you arrested? What is their agenda?
  + How much do they actually know?
  + How long can they keep you?

**4. Questioning Techniques**

Questioning techniques to be aware of include:

* Asking trivial information to get you talking and then shifting to more sensitive information when they feel you are co-operative;
* Threatening, then reducing the threat (known commonly as “good cop”, “bad cop”);
* Physical intimidation;
* Asking you the same questions repeatedly to see if there is any inconsistency in what you are saying. You may be asked to give the same timeline backwards to look for inconsistencies;
* Claiming that your co-workers or others have made allegations against you or that they have specific evidence against you. Their aim is to get you to confirm things they are suspicious about. Don’t voluntarily confirm what might just be their suspicions.

**5. What now?**

**Swipe right for this lesson’s checklist**

*RELATED LESSONS/TOOLS*

* *Travel Prep lesson*

*FURTHER READING*

* [*Good Practice Review Number 8: Operational security management in violent environments (Revised Ed.)*](http://www.odihpn.org/download/gpr_8_revised2pdf)
* [*ECHO Generic Security Guide for Humanitarian Organisations*](https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCEQFjAA&url=http%3A%2F%2Fec.europa.eu%2Fecho%2Ffiles%2Fevaluation%2Fwatsan2005%2Fannex_files%2FECHO%2FECHO12%20-%20echo_generic_security_guide_en.doc&ei=kLxAVc6LOILuUP2SgbAE&usg=AFQjCNEXEOcbLeV24f3WolHmDwLq7KJzlQ&sig2=hbnI7wfdrGIHS7mmikBRWA)
* [*Protection International: New Protection Manual for Human Rights Defenders (3rd Ed.)*](http://protectioninternational.org/publication/new-protection-manual-for-human-rights-defenders-3rd-edition/)

***Arrest Basic Checklist***

***Prevent arrest:***

* ***Maintain good relations with local authorities***
* ***Observe local laws and customs on and off duty***
* ***Carry correct legal documentation***
* ***Train and brief staff***

***If staff member is arrested:***

* ***Find out where they are held***
* ***Establish the facts***
* ***Engage a local lawyer***
* ***Advocate for their rights***
* ***Liaise with their family***
* ***Inform other organisations***

***If you are arrested:***

* ***Identify yourself***
* ***Inform your colleagues***
* ***Prepare yourself mentally***
* ***Stay calm***
* ***Do not give false confessions***
* ***Don’t sign anything you don’t understand***
* ***Request your legal rights***
* ***Be cooperative when appropriate***
* ***Don’t volunteer sensitive information***
* ***Establish the facts***
* ***Be alert to questioning techniques used***

**EVACUATION**

*BASIC*

**1. Phase One - Planning**

Evacuation planning and rehearsals should be carried out regularly. Security situations can deteriorate rapidly, often without warning. The evacuation plan should be prepared and all staff should understand an outline of it. The following issues should be considered when preparing your evacuation plan.

* **Under what circumstances will you evacuate?** Outline the situations and indicators under which you will put this evacuation plan into action. Identify the situations under which you will:
  + **Suspend** work activities in response to security concerns;
  + **Hibernate** by staff remaining where they are but keeping a low profile;
  + **Relocate** with staff moving internally within the country or to a safe-house to escape security concerns, or;
  + **Evacuate** with staff stopping work and leaving the country due to severe security concerns.
* **Who will be evacuated** - It is essential that all staff members clearly understand their and their families’ eligibility for evacuation or relocation assistance.
  + **Priority 1** – International staff family members
  + **Priority 2** – Staff members who are in immediate personal danger due to the conditions of the crisis
  + **Priority 3** – Individuals other than essential staff
  + **Priority 4** – Essential staff
* **Where will staff be evacuated to?** Identify a first-choice destination and an alternate destination for evacuation or relocation. Organise an emergency safe-house or safe-haven if needed. Determine visa requirements, and the logistics that will be needed upon arrival.
* **How will staff be evacuated?** Establish a notification system and an assembly point. Detail the route and method of evacuation. Check to ensure that these routes can be travelled under emergency conditions. Coordinate plans with embassies, UN agencies, and other NGOs as appropriate.

* **What goes and what stays?** Identify which documents, such as contracts, payroll records, etc. will be needed to re-establish operations once relocated or upon re-entry. Other documents should be marked for destruction, or left behind, as appropriate. Consider how evacuated documents will be perceived if seized by a particular person or group. They may contain information that could put those evacuating at risk, and would be better destroyed.
* **Who is responsible for the various tasks during an evacuation?** During crises key staff will be fully occupied so responsibilities for evacuation should be clearly defined during the planning stage.
* **What will be the expected impact of evacuation on the operation?** Will the office be closed and, if so, how? What are the policies and plans for continuing operations through national staff members acting on their own? Or through contractors, if feasible and appropriate?

**2. Phase Two - Alert**

Mounting tensions and/or instability may lead you or your organisation to issue a recommendation to limit operations, increase security measures, and review the evacuation plan. Work outside the immediate vicinity of the field office may be suspended. Tasks during this stage include the following.

* Brief all national and international staff on the situation.
* Communication systems for notification of staff should be finalized and tested. Consider tying into other systems, such as warden systems for other NGO, UN or embassy staffs.
* Prepare salaries and other money required by national staff.
* Back up important files onto disks, delete sensitive files, and destroy sensitive documents. See how to properly back up and delete files in the **Backing Up** and **Safely Deleting** lessons.
* Staff members and their family should check that they have personal documentation with them at all times.
* Inventory all office equipment and assets. As appropriate, identify the equipment to be evacuated and responsibility for each item. Plan how high-value equipment which will remain should be hidden or protected.
* International staff families should be considered for an early departure
* Potential evacuees should assemble personal belongings in grab bags to be taken during an emergency evacuation. See the **Protective Equipment lesson** for details on what to pack in a grab bag.
* Potential evacuees should ensure that they do not take with them any information or equipment that might be interpreted as incriminating (e.g. reports of military movements; pictures on disk or paper of any security-related subjects).
* Stock the safe-house or assembly area with appropriate supplies (Outlined in safe house section)
* Assign each evacuee to a specific vehicle so that anyone missing may be readily identified, and ensure that all vehicles are ready.

**3. Phase Three - Evacuation Imminent**

When evacuation is imminent the office should usually suspend most normal operations to concentrate on evacuation preparations. Potential evacuees may be relocated to a pre-selected safe area, or work from home. Remote staff should be recalled or relocated. Staff currently outside the region should remain in a safe place. Non-essential personnel and family members may be evacuated. Tasks during this phase, which may last weeks or only a few hours, include:

* + Keep all staff fully informed.
  + Coordinate closely with embassies, other NGOs, the UN, and other agencies as appropriate.
  + Pay salaries to local staff, with salary advances if possible
  + Hide high-value property which will remain. Remove any organisation logos from vehicles which may be stolen. Ensure you keep copies of serial numbers of high-value equipment.
  + Give clear instructions regarding responsibilities and leadership roles to those staff staying behind. Establish a means of continued communication between remaining staff and those evacuating. Provide authorisation documents to key national staff, if necessary.

**4. Phase Four - Evacuation**

Once evacuation or relocation has begun, it should take precedence over all other activities. The field office may continue operations through national staff, or contractors if appropriate, or may close completely. Considerations during evacuation may include:

* + If there is a risk of looting, consider disabling radios, equipment and vehicles. Empty and leave open all safes.
  + Ensure effective communication with national staff left behind.
  + All evacuees move to pre-designated assembly area.
  + Evacuate by the safest means possible, maintaining good order and remaining in communication with all groups evacuating.
  + Once evacuation is complete, inform HQ, relevant embassies, and key national staff.

The evacuated personnel may manage operations from outside the country, communicating with and working through the national staff (or contractors) if possible. If a decision is made to close the office completely, care will be needed to ensure humane and correct termination or reassignment of staff contracts and the disposal of assets.

**5. Safe-houses**

Safe-houses take a number of different forms. They can either be emergency safe-houses which are houses or apartments rented specifically for this purpose OR emergency safe havens which are in the already-occupied houses or apartments of friendly people.

Safe-houses and safe havens should be in a relatively anonymous community where neighbours won’t be suspicious about what is going on, or in a community where the neighbours can be relied on not to inform.

Safe-houses and safe havens should be in locations which allow observation of approaches to the property. There should be a number of emergency escape routes which are known to all those who may need to stay there. They should ideally have a secure parking place which would make it harder to place a tracker under the car at night. Safe-houses should be secure, with locks on windows, doors and gates and have a good quality alarm system and/or a dog. They should have a modicum of comfort – with appropriate running water, heating and electricity.

Safe-houses that are usually empty should be regularly serviced. Houses should not be left empty for weeks/months on end, as this may look suspicious: post should be collected regularly; the grass should be cut. If the house is unoccupied, non-sensitive activity should occur in the house every few days to make it look occupied. Ideally all rent and bills should be paid using cash to avoid leaving a trace.

Safe-houses and safe havens might need the following:

* Sufficient supplies of fuel, food, batteries and water for each person to last for a minimum of ten days.
* Emergency generator
* Battery or wind up mechanical radio and ideally a TV
* Clothing, especially outerwear appropriate for varying weather conditions
* Advanced first aid kit with necessary medications as required
* Flashlights with extra batteries
* Maps and communication plans as appropriate (to plan for emergency evacuation)
* Fully charged mobile phones and chargers, appropriate credit
* Satellite phone and charger (if issued)
* Sufficient amounts of extra cash
* Items to reduce psychological stress upon anyone using the safe-house (e.g. books, magazines, board games, games consoles etc.)

All sensitive waste produced at the house should be shredded/ securely burnt and disposed of. Residents should be aware of all possibly incriminating evidence that may be held there: electronic equipment; documents; travel tickets; receipts; or general waste which indicates the number, type or activities of the people using the house.

Emergency grab bags for each person should be located close to the most likely emergency escape routes. See the **Protective Equipment lesson** for details on what to pack in a grab bag.

**5. Considerations**

An evacuation is not easy for the evacuees or for those staying behind. It is a very emotional event, giving rise to feelings of guilt, hurt, frustration, and powerlessness. The departure of international aid organisations can have a variety of meanings to the local population, including the removal of a symbolic or real safety barrier. Thus, an evacuation is not a neutral act and may even aggravate a crisis. When a field team evacuates it should consider providing a statement for the media and others explaining the organisation’s reasoning and any continuation or possible resumption of programmes.

**Self-evacuation.** Individuals that are working remotely from a local office, or who find themselves isolated during a crisis should use their judgement concerning the safety in their area. All staff members should be authorised to evacuate on their own authority when they feel their safety is threatened, and should communicate with their manager during the process.

**Evacuation refusal.** Staff who are instructed to evacuate or relocate, and who refuse, may face disciplinary action. They are likely to be considered as staying at their own risk.

**National staff evacuation or relocation.** Many humanitarian organisations have a policy of only evacuating international staff. If the manager believes that some or all national staff and/or their families face a direct threat, then they should consider organising or assisting their evacuation or relocation.

**Return and resumption of activities.** This may occur soon after evacuation or take a long time. Re-establishing operations after an evacuation can be difficult. National staff who did not evacuate may have experienced hardship and threats to themselves and their families and this can understandably cause tensions. Due recognition of their achievement is important. Restoring relationships with staff, local authorities, beneficiaries, and the local population can be made easier if honesty, tact, and transparency are used prior to and during the evacuation, and on return. Read the **Stress lesson** on how to help manage the stress of staff.

**6. What now?**

**Swipe right for this lesson’s checklist**

*RELATED LESSONS/TOOLS*

* *Baking Up lesson*
* *Safely Deleting lesson*
* *Protective Equipment lesson*
* *Stress lesson*

*FURTHER READING*

* [*ECHO Generic Security Guide for Humanitarian Organisations*](https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCEQFjAA&url=http%3A%2F%2Fec.europa.eu%2Fecho%2Ffiles%2Fevaluation%2Fwatsan2005%2Fannex_files%2FECHO%2FECHO12%20-%20echo_generic_security_guide_en.doc&ei=kLxAVc6LOILuUP2SgbAE&usg=AFQjCNEXEOcbLeV24f3WolHmDwLq7KJzlQ&sig2=hbnI7wfdrGIHS7mmikBRWA)
* [*Good Practice Review Number 8: Operational security management in violent environments (Revised Ed.)*](http://www.odihpn.org/download/gpr_8_revised2pdf)

***Evacuation Basic Checklist***

***Phase One***

* ***Plan the who/what/when/where/how of potential evacuation***

***Phase Two***

* ***Brief staff***
* ***Test communications system***
* ***Prepare all payments***
* ***Back up/ safely delete files***
* ***Staff and families should carry personal documentation***
* ***Prepare grab bags***
* ***Stock the safe-house***
* ***Inventory assets***
* ***Assign and prepare vehicles***

***Phase Three***

* ***Keep staff informed***
* ***Coordinate with embassies and agencies***
* ***Pay all salaries***
* ***Hide high-value assets***
* ***Remove logos from vehicles remaining***
* ***Give clear responsibility to staff staying***

***Phase Four***

* ***Consider disabling equipment***
* ***Leave safes empty and open***
* ***Ensure effective communication with national staff***
* ***Evacuate by safest means possible***
* ***Upon evacuation, inform national staff, embassies etc***

***Safe-houses***

* ***Should be secure building in safe neighbourhood***
* ***Should be lived in / serviced***
* ***Should be stocked with emergency goods***
* ***Waste should be securely disposed of***
* ***Grab bags should be placed by escape routes***