SECURITY GUIDELINES

FOR HUMAN RIGHTS DEFENDERS

WDD
WHO DEFENDS DEFENDERS?

This project is funded by the European Union

Impressum

Published by
Civil Rights Defenders

For publisher
Goran Miletic
Director for Europe

Author
Pavle Petrovic

Translation and proofreading
Anica Milenkovic
Zorica Radic

Design
Marko Kovachevski

Printed by
Zeppelin Pro

Number of copies
100

ISBN:
978-86-89531-05-3

SECURITY GUIDELINES

FOR HUMAN RIGHTS DEFENDERS

2019/2020

INTRODUCTION

THE ORIGIN AND PURPOSE OF GUIDELINES, CURRENT SITUATION REGARDING NGO AND JOURNALIST SAFETY IN SERBIA

The security of non-governmental organisations in Serbia is more specific than security of commercial or, for example, government organisations. The most conspicuous characteristic is the complexity of threats the non- governmental organisations are facing, because they come from a broad range of sources The most conspicuous characteristic is the complexity of threats the non-governmental organisations are facing, because they come from a broad set of various threat sources.

For a short period of time, a non-governmental organisation would be exposed to threats of right-wing supporters' vandalism, negative tabloid campaign against its activists, open threats on social media and officials' statements labelling the NGO's activists. Such various threats create the synergy of threats, which require serious and dedicated approach from the organisations, but at the same time represent a new item in their budget.

Since non-governmental organisations lack a habit of dealing with issues of security in a systematic way, by now they reacted to threats mostly depending on the situation – by developing parts of the security system only after they suffered some threat. It is of the utmost urgency to change this kind of approach.

On the good side, the NGOs established good communication between the organisations by dealing with security problems so far, and this manner helped us to learn from each other through situational responses. It would be good to nurture this habit and if possible, utilise it even more by converting the experiences we had exchanged into useful procedures.

If the former approach to security is not changed, there is reasonable fear that threats will become the main preoccupation simply because there will be more and more threats. Such a problem would heavily overwhelm the daily activities of NGOs and their activists would be working in an atmosphere of fear. Such a problem would heavily overwhelm the daily activities of NGOs and their activists would be working in the atmosphere of fear.

The goal of these guidelines is to introduce the non-governmental organisations' activists to the most frequent threats they might encounter in Serbia, their most frequent forms, methods of fighting them, and most importantly, how by developing safety plans and procedures we can develop the security system tailored to our needs. Many times repeated procedures, along with high level of vigilance (we will also discuss this) will in time build the safety culture at the level of the organisation and with every activist. Good safety culture can even compensate for the lack of resources and can create the biggest problems to the threat sources, whatever they are – and that is our ultimate goal.

ESTABLISHING PRIORITIES IN PLANNING SECURITY

We have mentioned that the situational response to already executed threats is the ‘reactive’ tactics of the majority of Serbia-based NGOs. Only after they shut down websites, NGOs consider hiring an IT expert who will take care of the server security, or organisations would install security bars only after the office doors are were broken into.

Contrary to this, to develop the optimal security system, we have to approach the problem systematically i.e. from the beginning. The beginning of security planning is that we must preserve our values – both of the organisation and the activists. Some of the values are universal, such as the physical integrity of the activists, integrity of the office and reputation of the organisation, i.e. these are specific for all organisations. Depending on the organisation’s activity, those values can further be physical archives with the documentation, integrity of the server, undisturbed street action or performance. To make this list final these are the questions we must ask:

What is necessary for organisations to function?
What is necessary for organisation sto function as we have planned?
Which fundamental values of activists the organisation can protect?

The best would be to write down the values we came across by answering these questions separately in the table, because this would facilitate further planning.

Undisturbed organisation of an event
Physical integrity of journalists/activists
Life of journalists/activists
Material equipment (outside the office)
Organisation’s reputation
Reputation with donors
Particular donor’s trust
Feeling safe in our events
Our reputation with the readers/supporters

We will attribute a score from 1 to 10 to the values we have enumerated. We will imagine that specific value is threatened and then we will attribute it a number which should describe to which extent the organisation and activists would suffer if that value would be threatened. The number will represent the assessment which we will define as **“critical importance of values”.**

Score 1 or 2 is for the values which when threatened will not affect the life and health of activists/journalists, but will have a minor effect on the work of the organisation. Here we can put values such as “good Internet connection”.

Score 3 or 4 will be for values which when threatened will not affect the life and health of activists/journalists, but can significantly affect the work of the organisations, if the damage occurred can be relatively soon removed – for example, it will slow down the work of the organisation for a short period of time. This assessment is for values such as “the list of activists” or “the access to the website” (if we are not the web portal).

Score 5 or 6 will be for values which when threatened will cause damage which will require additional effort to be repaired (sometimes outside the capacities of our organisation) and will stop the work of the organisation for a short period. We are not talking about health or human lives. These values may be “undisturbed organisation of an event” or “particular donor trust to our work”.

Score 7 or 8 is for values which when threatened may stop the work of the organisation for a longer period of time. This can be “our reputation with the readers” (if we are the web portal) or “financial documentation”.

Score 9 or 10 is attributed to most important values, such as lives and health of our people or some persons who if threatened or ended up in danger will mean that the work the organisation will stop completely. So in addition to aforementioned physical integrity of our activists/journalists, here we also refer to anonymity of the secret source (since their physical integrity depends on this directly), as well as reputation with donors or long-term financing of the organisation.

Undisturbed organisation of an event	5
Physical integrity of journalists/activists	9
Life of journalists/activists	10
Material equipment (outside the office)	5
Organisation’s reputation	9
Reputation with donors	9
Particular donor’s trust	5
Feeling safe in our events	6
Our reputation with the readers/supporters	8

After determining the critical importance of values, we will mention as many potential threats as we can to the organisation and its employees. When enumerating potential threats, we will keep in mind that here we only deal with threats that an organisation can influence and that concern its work, so we will not refer to threats that employees as individuals can face, if those are irrelevant for their work in the organisation.

To list all the threats, we should start from values that we have mentioned before. For each value we should think of at least one potential threat, so for the value “undisturbed organisation of an event” we will mention the threat “counter-protest”, “assault on activists during the event”, “police ban of the protest”, and others.

We will put the list of threats in a separate *excel* sheet, and next to each threat we will put the score we have previously determined as level of critical importance of values – for the value threatened by specific danger. If several values are threatened by a single danger we will put higher critical importance of values.

For example, “counter-protest” threatens “undisturbed organisation of an event”, which had critical importance 5. So in this sheet next to “counter-protest” we will put 5.

However, “assault on activists during the event”, in addition to threatening the value “undisturbed organisation of an event”, also threatens “physical integrity of participants of the event” which was assessed 9 or 10. In this case next to a threat “assault on activists during the event” we will put 9 or 10.

THREAT	SEVERITY
Counter-protest	5
Violent interruption of the event	9
Police ban on the event	7
Physical assault on an individual outside the office	9
Physical assault during the organisation of an event	9
Seizing of equipment	5
Stolen equipment	5
Negative campaign in the media	9
Negative social media campaign	9
Unprofessional behaviour of journalists	9
Non-compliance with the procedures agreed with the donor	5
Poor choice of partner(s) for project realisation	9
Intimidated supporters	6

Then next to each threat we will write down as a percentage the probability of specific threats occurring within a planned period. A Planned period is the period of time for which we are developing our safety plan. It can be a five-year period, but for large organisations and periods of intense developments concerning security, we can make annual safety plans.

Concerning the probability of some threat occurring within the planned period, we will take following items as references:

- History of those threats occurring for our organisation
- History of those threats occurring for organisations similar to ours
- Statistics of threat probabilities which some security related NGO had collected
- Statistics of threat occurrence published by some government institutions (police, prosecution, courts and other)

There are no clear rules when it comes to probability of some threat occurring in the planned period, yet if our organisation had already experienced this threat in the previous period (let’s say a five-year period), and none of the circumstances changed in the meantime, then it is highly likely that the threat will occur. It is less probable that threat will be repeated if we have not experienced it, but other organisations had.

We will put these three parameters (threat name, highest critical importance and probability of occurrence within the planned period) in the *excel* sheet with the function of multiplying the probability and critical importance of values. We will get the final assessment, which will indicate the biggest threats to our organisation.

THREAT	PROBABILITY (%)	SEVERITY (0-10)	SCORE
Counter-protest	100%	5	50.00
Violent interruption of the event	90%	9	81.00
Police ban on the event	10%	7	7.00
Physical assault on an individual outside the office	50%	9	45.00
Physical assault during the organisation of an event	90%	9	81.00
Seizing of equipment	40%	5	20.00
Stolen equipment	40%	5	20.00
Negative campaign in the media	100%	9	90.00
Negative social media campaign	100%	9	90.00
Unprofessional behaviour of journalists	40%	9	36.00
Non-compliance with the procedures agreed with the donor	10%	5	5.00
Poor choice of partner(s) for project realisation	30%	9	27.00
Intimidated supporters	90%	6	54.00

After this, all threats with the final score of over 50 will get our special attention and we will use them to create **threat analysis**.

Threat analysis shall be a document that we will use as a foundation to further develop our safety system – we will know the direction of our further training, in which equipment we will invest the most and which procedures development will occupy our greatest attention. The most important thing – threat analysis is the foundation for development of **safety plans**, which we will discuss by the end of these guidelines.

Threat analysis is developed as a specific table for each threat separately, and in addition to the name and short description of the threat, it shall include the following elements:

- **Consequences** – in addition to direct consequences to our organisation's values and employees, we will mention other consequences – usually "domino effects", i.e. influence on causing new threats;
- **Objects of threat –** helps us recognise which values will be threatened after the threat was realised;
- **Threat sources** – list as precisely as we possibly can all potential organisations, individuals and natural hazards as threat sources concerned;
- **Strength and capacities of the threat source** – list the advantages of threat source; e.g. support of the major part of the public, abundance, physical strength, etc.
- **How** is the threat realised, i.e. what actions the attacker must take so as to realise the threat; this is especially important with complicated threats;
- **Where** the threat may be potentially realised – list all potential places where the threat might be realised;
- **Our capacities** – all potentials we as an organisation and as individuals have at our disposal, which we can use to fight threats;
- **Our weaknesses** – all former bad practice, lack of safety equipment or lack of discipline that the attackers might turn into their advantage.

Example – threat analysis

THREAT	Counter-protest						
Short description	If we organise a public event in our premises (promotion, panel discussion, projection and other), it is highly likely that right-wing and extremists groups will organise a counter-protest at the same time in front of our office so as to disturb or try to stop our event.						
What	**Object of threat**	**Threat source**	**Power and capacity of threat source**	**How**	**Where**	**Our capacities**	**Our weaknesses**
Explain what might happen if the threat is successful (if necessary divide a threat into several components)	Who / what is the object of threat?	What entity is the threat source?	Describe which resources, skills and capacities the threat source owns.	Which information/ actions are necessary so the threat would be realised?	What is the potential place where the threat might be realised?	Which existing procedures and capacities can reduce the probability and impact of the threat?	In relation to our threat, what are our weaknesses?
If the counter-protest would be organised, these might be the possible scenarios: - cancelling the initial event - disturbing the course of project activity - physical conflict might occur - material damage - loss of audience, sympathisers who can be intimidated during the threat - negative "points" with donors	Everyone present. Organisers, citizens who came to the event, material property of the organiser.	Right-wing organisations, extremists organisations, individuals – opponents	No criminal penalties after the incident. Support of some political parties and a part of the public. Number of people and level of preparedness. Amount of information on our activists / journalists as well as activities.	Monitoring the work of our organisation when it comes to public invitations on events, promotions and activities. Organising counter-protests – inviting their members and supporters to counter-protest.	In open space in front of our office, in front of conference halls and movie theatres.	Inform the police about the public events. Drawing the attention of the public – reporting from counter-protests.	For a longer period of time, we have been marked as a threat through campaigns against the individuals close to our organisation or against the very organisation. In front of our office there is public space where it is easy to organise counter-protest.

TYPES OF THREATS THAT NGO's AND JOURNALIST IN SERBIA ARE FACING

There are various types of threats that non-governmental organisations in Serbia are facing, and persons making threats are usually driven by either hate or authorities' interest, and the threat sources are typically related to far-right political ideas. The ultimate goal the persons making threats are trying to achieve is to reduce the influence of non- governmental organisations, through various attempts of intimidation and degradation of the organisation's reputation.

THREATENING PHYSICAL SAFETY

AN ASSAULT ON AN INDIVIDUAL

In Serbia, it is not unusual that activists and journalists are physically assaulted. Here we mean assaults on individuals, outside of their working assignments, which are planned (for the purpose of intimidation) or caused by uncontrolled emotions (reaction to previous targeting). The consequences of an assault, in addition to injury and potential serious consequences, also make an impact on more values – the morale of the individual and the organisation, and also further targeting of other activists as legitimate targets of physical assaults.

A physical assault on an individual (activist or journalist) may be either planned – if someone ordered it, or situational – as a direct consequence of targeting that person or the organisation he/she is actively engaged in.

Planned attacks usually carry a 'message' of the person who ordered the attack, and the message is that activists/journalists should stop with their activities which concern those who ordered it. Those can be politicians who are under media investigations, businessmen who believe their jobs are at threat or war criminals because we drew attention to their media rehabilitation. Perpetrators of these attacks are usually paid-criminals, or sometimes even bullies who commit the attacks out of 'party duty'. Even in most detailed planned attacks, the perpetrators may appear as either fanatical citizens or right-wing parties' activists.

Before **situational attacks** we almost always have targeting of activists or entire organisation through tabloids, social media or public persons' statements – mostly politicians. After activists are labelled in public as "traitors" or "foreign mercenaries",

bullies will decide "to defend justice" or will attack activists when they recognise them. These attacks can be more dangerous since they can escalate and rise to proportions that the perpetrators had not even planned.

In addition to useful procedures that organisations may introduce for the purpose of fighting these types of threats, it is even more important to take care of personal safety.

- When it comes to personal safety the fundamental principle is **the level of attention** we pay to our environment at any given moment. An appropriate level of attention means that at the moment when we are exposed to various risks we are completely observant of our environment and the part of our attentive behaviour is directed to noticing potential attackers. This means **that at moments when we are vulnerable** (getting in or out of office/apartment/car, when we are moving down the empty or dark street without any people or light, and other) **we must not look at our phone, listen to music or look down.** To direct our attention properly, we need to know how these attacks look like, and this is why it is important to get informed more on all cases of attacks on journalists. If we are attentive enough we may notice being tailed or watched in time, because these are preconditions for attackers to organise kidnapping or make life threats. When we are attentive we can notice the attack in time, so we can react quickly. So, the preconditions of personal safety are focus and familiarity with the environment.

- Next important thing is **to observe, recognise and report when someone is tailing you or watching you** because those are, as we have mentioned before, attacker's necessary preparatory actions for the forthcoming attack. Government security service tailing is more hard to notice than being followed by criminals, mercenaries or political groups, but you can still notice it if you are familiar with this area and vigilant enough. If you notice you are being followed, **it is necessary to report that to your editor / organisation director, and if necessary to the police**. Later we will discuss secret following (tailing) in detail.

- It is also important **that you are ready to fight your threat**, i.e. to defend yourself. Confronting your threat does not mean that you are necessarily responding with violence, yet there are many self-defence techniques, fast flight from the attack scene, signalisation in case of kidnapping and escaping if you are secretly followed. You may find the following pieces of advice helpful:

  - Try to wear clothes and shoes which allow you to run, stay fit so you can run and avoid blind alleys. Always be aware of potential exists from the room or the street you find yourself in.

  - Practice some self-defence sport and carry some legal self-defence weapon (e.g. pepper spray).

- In case of danger, walk quickly towards the public place. Get inside the first café and ask the staff to call the police.

- Walk your dog and keep a dog in your backyard, if you can.

- If there is risk of kidnapping, use an emergency tool so you can inform someone about your location, and if you do not have this carry something with you that can make noise (e.g. a whistle). Even better option is to loudly cry “help” or “police”. Whenever you can, inform your friends, family or colleagues in advance about your whereabouts.

- Walk as closely as you can to buildings with security, and if you are taking public transport, sit closely to the driver.

- Park your car in well-lit spaces and check you back seat whenever you are getting back to the vehicle.

- When approaching your car or your apartment, get your keys on time. It’s a vulnerable situation, so this should reduce the time you are standing in front, and at the same time you can use your keys for self-defence.

- Carry your computer or your documentation with you only when necessary, and keep you phone in a safe place. The attacker might target some pieces of your equipment in order to obtain data on the story you are working on.

- Do not share too much personal information on social media. This primarily means information on your current location, where are you planning your journey or photos of your apartment interiors.

PHYSICAL ATTACK OF ORGANISATION’S OFFICE (VANDALISM)

Vandalising offices of NGOs in Serbia is quite frequent, especially NGOs that work in protection of human rights. The goal is to intimidate the activists and put stigma on NGO and activists as ‘traitors’ or ‘mercenaries’. The only certain consequence is material damage, but vandalism can make new followers walk away and influence current activists’ morale.

Most frequent form of vandalism is writing graffiti on the front doors, smashing windows and glass doors of NGO office. Rarely, the attackers will get inside the office and further destroy the equipment. Vandalism is usually carried out by attackers in groups, outside working hours and sometimes they would use public rallies because they believe they will remain undetected.

To protect against vandalism, the most useful advice shall be:

- Installing security cameras that cover all areas that could be vandalised – front doors and glass tops exposed to potential attack; if the organisation does not have enough money to cover costs of camera installation, it could be useful to install fake camera, which is much cheaper and will serve to discourage vandals (they will be afraid they will be recorded);

- Installing protective foil on glass tops that might be exposed to potential attacks; this is protective foil against glass smashing (glass might crack during the attack), which will prevent office interiors from further attacks; this is a more efficient and aesthetically more acceptable solution compared to e.g. security bars or roll-up doors, if vandalism is the main concern.

- When choosing your office location make sure it is inside the well-lit street where majority of stores or institutions have video surveillance that covers the street; if your office is inside the building (there is no direct access to the street from the office), make sure that intercom and front door lock are well-functioning, and the hallways are well-lit – potential attackers will find this unappealing;

- Informing the public on all attacks and, when necessary, publishing the identity of the attacker (if we know the attacker).

ATTACKS ON ACTIVISTS DURING STREET ACTIONS

Attacks on activists during street actions usually occur during counter-protests organised by groups of attackers or, less often, when spontaneously carried out by “revolted” passers-by. The goal of these attacks is to stop the actions, intimidate and discourage activists, and the long-term effect is the “militarisation” of actions. This shall mean that, due to frequent attacks, the actions might get strong police protection, which, although increasing the level of security, will potentially reduce the visibility of actions, negatively affect the mood of current and future activists and appear to general public as “spending budget money”. In addition to thinking about the safety during the action, we should pay a lot of attention to the preparation of the action because of all this, and all methods of discouraging the attackers.

With this in mind, we can list several useful recommendations:

- Before implementing street actions we have to remind all activists to agreed behaviour during action, and what would be the favourable response to provocations of counter-protest participants. Usually that would be composed behaviour towards counter-protest participants and non-responding to their provocations. The most important thing is that none of the activists will act alone, especially in relation to the counter-protest participants – in case of all kinds of attacks we should all stick together.

- Moreover, before carrying out street actions, we should examine in detail the route we are taking, the transport means and most importantly, the route and manner of pulling out in case of physical attack.

- If it is an action where surprise factor is not that relevant, we will inform the police about the rally, and then we will follow all their recommendations regarding safety.

- If the surprise factor is really relevant for this action (e.g. protesting on the event paying tribute to war crimes), we will make sure to protect secrecy when organising the action. We will maintain secrecy if we use the app *Signal* for phone communication, and if we are not posting on social media, and we are not informing the persons not participating in the action about it.

- If we know there is great risk of physical assault during action, we will consider taking self-defence weapons with us (first of all pepper spray), and it is desirable to carry first aid kit. Within that sense, it is desirable to develop and maintain self-defence skills and giving first aid.

SECRET SURVEILLANCE

Secret surveillance is secret information gathering (intelligence) about movement of persons, their habits and contacts they make. Persons are tailed (on foot and by vehicles) or monitored by using technical instruments (such as GPS locators and mobile phones). In this part we will discuss more about physical monitoring. Attackers may carry out secret surveillance due to many reasons, but one can say the most general reason is almost always gathering information (intelligence).

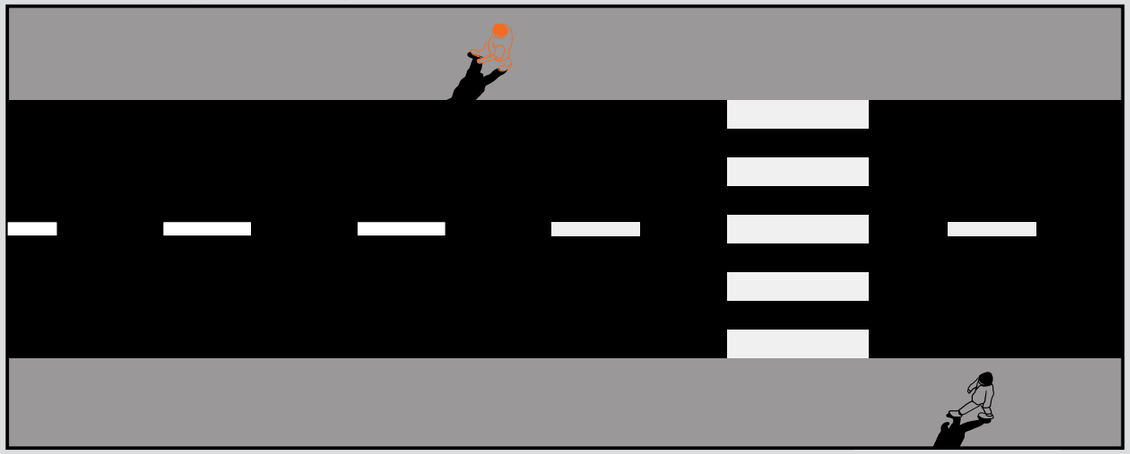
Ultimate goals of secret surveillance could be the following:

- Gathering information on movements and habits of person being followed – this is often done before taking other actions, such as:
  - wiretapping and photographing private and business meetings
  - secret search of office or apartment
  - gathering discrediting data
  - physical assault or intimidation
  - stealing or snatching equipment (primarily data carriers – laptops, phones or documentation)
  - kidnapping
  - assassination
- Gathering information on private and business contacts of the person being followed, carried out for the purpose of:
  - Disclosing secret journalist's source or a whistle-blower,
  - Disclosing partners in project,
  - Recording discrediting material.

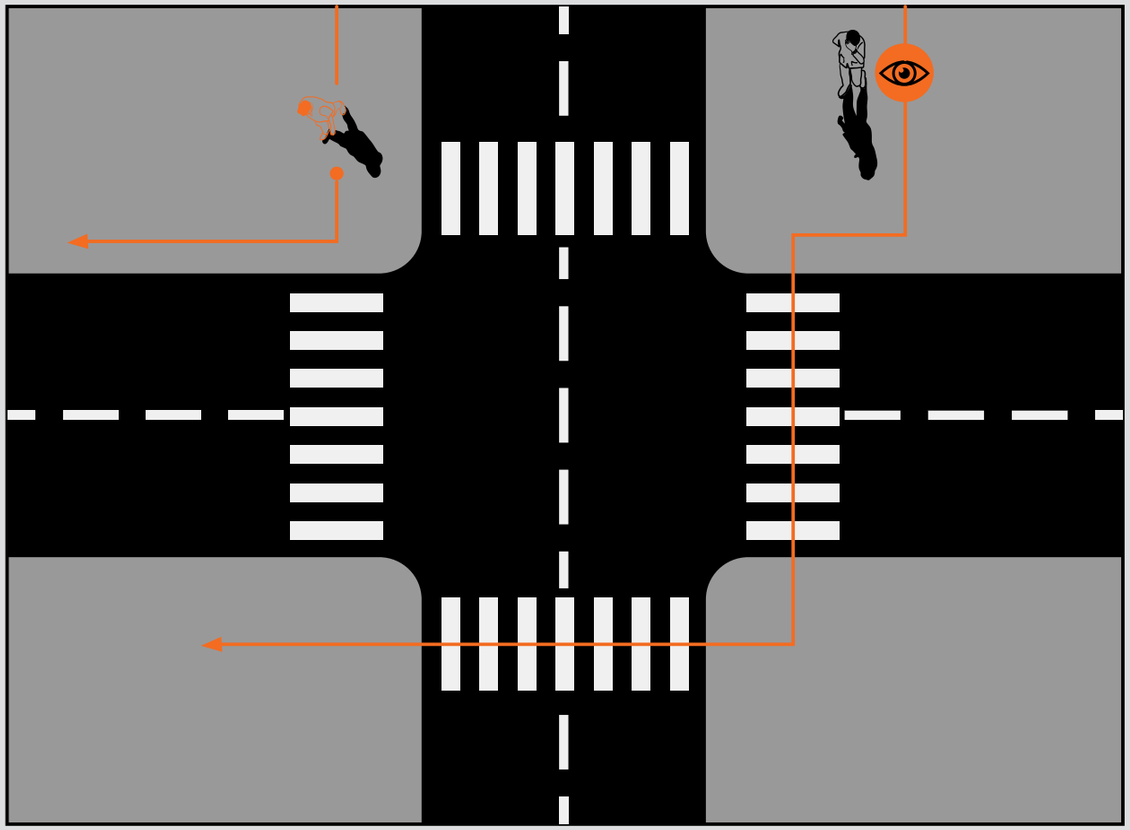
Secret surveillance could be carried out by anyone with a purpose of realising some of the aforementioned goals, in majority of cases by members of secret service and the police. In other potential circumstances the surveillance could be carried out by paid professionals/private detectives, members of criminal groups, and rarely, better organised extremists groups.

For us to recognise the secret surveillance, it is important to know its rules:

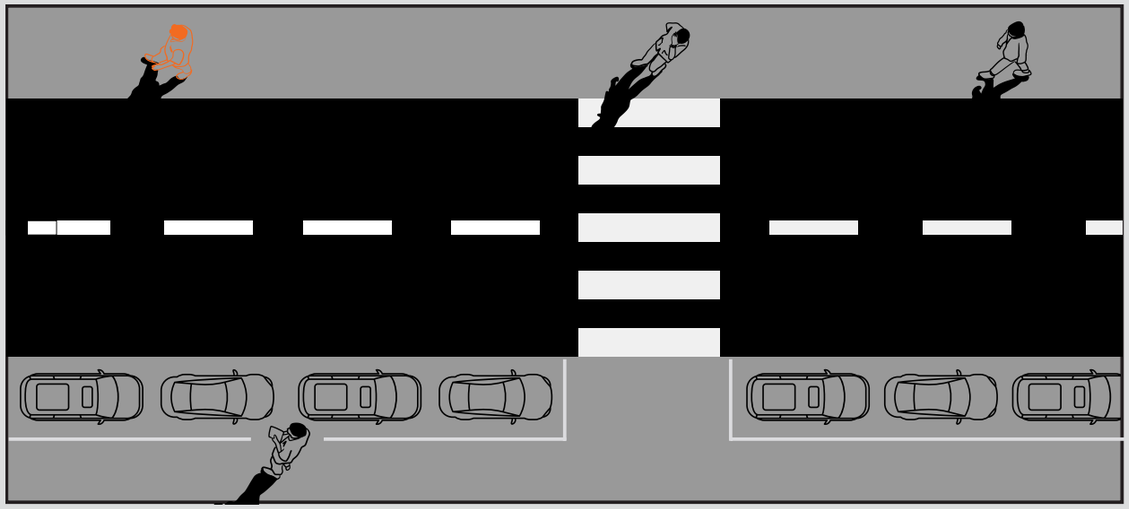
◆ The person secretly following us will unlikely have conspicuous appearance.
◆ The person secretly following us will not wear flashy clothes and will probably wear jeans and dark top/jersey.
◆ The person secretly following us will usually walk on the opposite side of the street from the person being followed and of course behind them too.



◆ To maintain the previously mentioned principle, persons from secret surveillance, when we turn right at the crossroad, will awkwardly bypass the crossroad and continue behind us, but still on the opposite side of the street.



◆ Other persons from secret surveillance (not those closest to us, i.e. right behind us), in case of street tailing, will be right behind the first person from the surveillance, but on your side of the street (behind the other). Persons from surveillance could switch in agreed intervals, at usual places or if need arises – when first person from surveillance is "spotted".

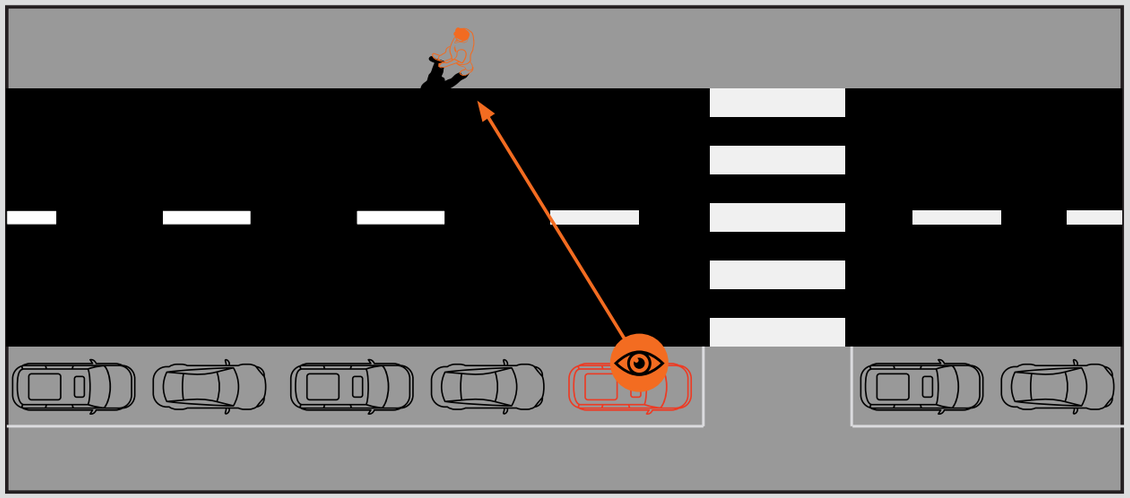


◆ Secret surveillance will apply “elasticity principle”, meaning that the person from the surveillance team will be closer to the person being followed when in a crowd (not to “lose them”) and keeping greater distance when there are few people in the street (not to get suspicious).

◆ Secret surveillance will apply the “box principle” when the person being followed ends up in an area without defined streets where they could easily “ditch” the secret surveillance (park, shopping mall floor, green market, and other). In such cases persons from secret surveillance (there should be at least three in this type of situation) will take such a position that the persons being followed will get surrounded by them.

◆ If a person being followed stops or gets inside some store, the person from secret surveillance will take the beneficial position opposite from the store (so-called **shelter**), where they will wait for the tailed person to appear. The Person tailing you will get inside the building behind you if they know or assume that building has another exit that you may use to get out or if they fear you might meet someone inside the building. For you to recognise that someone is taking shelter, we will mention what would be the most important characteristics of a good shelter:

- The shelter to be taken by a person tailing you will be across the building entrance, but not directly across, yet diagonally. Apart from the building, the person tailing you might use the parked cars as well.



- The shelter must always have good visual overview of the surroundings – in that sense the best option are shops with big widows, and the best are those on the corner with windows looking onto both streets.
- It is a kind of a place where you can stay long enough, if necessary – the person from secret surveillance will also consider and make an assumption how long the persons being followed will stay in the building they entered. For all this, a café can be a good shelter.
- That is a place from which a person in secret surveillance can move quickly and continue with tailing. Restaurants and other places where one has to wait to pay the bill can get awkward because of that. You can spot people from secret surveillance easily – if they pay the bill in a café/restaurant as soon as they get the order.
- That is not a busy place – long “mobile phone conversations” can be suspicious, so people from secret surveillance use them only if really necessary and if all other options fail.

How to resist secret surveillance? First and hardest thing is to recognise tailing. Only after we have noticed we are being followed, we can take additional steps. We recognise two forms of detecting secret surveillance – antisurveillance and counter-surveillance, and obvious and covert countering of secret surveillance.

Antisurveillance means that we can recognise secret surveillance by ourselves without others’ help. As we are identifying secret surveillance by ourselves, we should be highly trained and it is very challenging that we keep our identification of secret surveillance hidden. If we trained antisurveillance techniques well, the ultimate goal can even be to “lose the tail”, i.e. escape secret surveillance, which should be the least obvious to the persons tailing you.

Unlike the antisurveillance, **counter-surveillance** shall be done with the team assisting us to recognise the presence of secret surveillance. Unlike the antisurveillance that is situation-based (when we suspect of secret surveillance in the field), counter-surveillance is planned ahead – before meeting with your secret source or when necessary to absolutely prove you are being tailed. We will position members of our team along the route we will take – in the locations we have previously described as good shelters. Members of our team will try to detect all characteristics of secret surveillance – avoiding crossroads, “elasticity principle”, “box principle”, conspicuous behaviour and other. Members of the team should maintain good communication (favourably by encrypted correspondence – through *Signal* app) and exchange information on potential persons tailing them. Last member of the team distributed along the route, and on the basis of the information he/she received from the members strategically positioned in locations before him/her, must give the final judgement if there is secret surveillance or not, and they must report that to the person being tailed. On the basis of the final information, whether there is secret surveillance or not, the person being monitored will make the decision on whether, for example, they will go and meet their secret source.

Obvious countering of secret surveillance is based on recognition techniques that would be visible to persons tailing you, meaning it would be clear to them you have noticed them. Carrying out these recognition techniques is so much easier compared to covert techniques and in short term they can prove to be efficient – exposed person from secret surveillance can temporarily withdraw and for some short time ahead we might not have a person tailing us. In a long term, these techniques will cause us damage since members of secret surveillance will be clear that we are ready to resist and fight back, and they will send someone with more experience to tail us and it could be they will get better technical means and broader competences. Examples of obvious resisting to secret surveillance might be using unusual walking routes (for example, four times in a row at the crossroads we are turning to the left around the building or a block paying attention that someone suspicious is doing the same as us), crossing at a red light, evident stopping in the middle of the street or behind the corner, waiting on the top of escalator and strikingly watching everyone coming behind us and other. We can use these techniques when we suspect someone is taking our photos during the meeting in the public place – we can also openly take photos of the person we are suspecting is taking our photos by using our phone and pay attention to their reaction (if that person was really taking our photos, they probably won’t object and will ignore our reaction).

Covert (subtle) countering of secret surveillance should be done so the secret surveillance will not notice we have detected them and that, if we lose them, they will not realise we did it on purpose. Covert identifying of secret surveillance is much harder than obvious disclosing of secret surveillance, but if it was really well-trained and remained undetected, we will gain much more advantage. After performing such disclosure of secret surveillance we do not have to worry that secret surveillance will significantly increase their presence. Examples of

good covert countering of secret surveillance could be using mirror (or shop windows) so we could detect potential followers behind us, then intelligent using of blind alleys (pretending we have walked into a blind alley by accident, and then going back and noticing who walked behind us), discreet observation of avoided crossroads, taking good shelter and other rules related to secret surveillance.

We can, after all this, give you some practical advice to help you notice the secret surveillance:

- Remember all suspicious persons whose conduct appears to follow the rules of secret surveillance we have mentioned. When we remember the appearance of suspicious persons, we should try to memorise their height, figure and the way they walk, and their pants and clothes (this is something it is hard to change in the field). Ignore the details such as hat, scarf, glasses, and beard and moustache too– this can be modified easily.

- Pay attention to people looking out and looking to your direction several times. Don't take this as evidence, but that could be a good indicator who might be suspicious when you start recognising the secret surveillance.

- Monitor reactions to your actions, especially after you have spoken to a person. For example, if you suddenly address a person with a question about some street location or what time is it, if that is person tailing you, you can expect they will get confused or start panicking.

- Pay attention to people who do not fit the environment, meaning they found themselves there only to tail you. In such a situation persons tailing you might find themselves in places where they do not belong, judging by their sex, age, clothes or appearance in general, which might be easily detectable in a given situation.

- Pay attention to persons taking good shelters – those who have parked diagonally across the entrance to you building or the office, who entered the shop across the one you have just entered or have stopped at the same moment you have paused and stopped.

- Any kind of unusual behaviour is a good indicator that this person was sent to tail you – if that person sat alone at the table in the café where you are to meet your secret source or had tried to get inside the building behind you (you kept the door for them), and later on it turned out they did not have the key to front door, and other.

- One of the resistance methods could be to get "boring" if you assess that you have person tailing you only to collect data on the case you are currently working on. This means that for next ten days you should refrain from actions that you presume the secret surveillance is interested in. In that case they will have nothing to gather and probably in the following period they will stop monitoring you.

- If you can keep it unnoticed, then you can create a photo stock of people you are suspecting are tailing you. The best thing would be to share this stock with other people so they can use it later on for identifying persons who could make some serious threats.

- In the end, when you notice someone is tailing you, take that really seriously. Although there are number of reasons someone would be tailing you, it is always the most useful to take it as a serious threat to personal safety. Depending on the situation, this threat should be reported to the editor / programme director, and if necessary to the police.

THREATENING INTEGRITY OR CONFIDENTIALITY OF INFORMATION

PHONE TAPPING

When exchanging any kind of confidential information, never do that over the phone unless you are doing it through a encrypted communication app. The goals of gathering information in such way are very similar to secret surveillance – first of all, gathering information on your activities, routine collection of data on your habits and contacts, but also discrediting material.

In addition to the government, private companies and political parties could have required resources to monitor activities on your mobile phone, and they are willing to infringe the law so as to obtain information on your work and private life. Conversations on the landline phone are usually monitored only by public authorities.

How someone can use your phone to gather information on you:

- Intercepting and recording conversation you are having on your landline and mobile phone, which is mostly done by government services with the help of phone operators;
- Collecting listings of conversations from landline or mobile phone and exchanged messages, which means less legal "obstacles" for those carrying out this type of monitoring;
- Collecting files from mobile phones; this usually occurs with the authorisation of the phone owner since the majority of applications we install require permission to access files on the phone, but this occurs during the installation of viruses as well;
- Collecting data on physical movement of the phone, which again usually happens with our consent since we provide authorisation for phone geo-location to various applications, but this could be done if we install the virus; the information on the phone geo-location could be obtained retroactively by using government resources, and/or telephone operator resources as they possess data that is recorded if phone was anywhere near the base stations;
- Access to complete content of your phone – conversation monitoring (whether through standard phone line or through some app), access to files stored in phone, monitoring movement (geo-location) of the phone; some viruses can even track communication taken over app for encrypted communication, and can abuse our microphone and camera even when we are not using them.

When we know which possibilities the attackers have we can give some practical advice:

- You should not talk about confidential matters over standard phone line. When assessing what is confidential, ask yourself following questions:
  - If disclosing that data and its availability to some interest group or public can harm my organisation?
  - If disclosing that data can harm my phone interlocutor and their organisation?
  - If data we are disclosing indirectly indicate the identity of secret source or can disclose some particularly secret information?
  - Are we disclosing something in conversation that could be used for our discrediting?
  - Can conversation recording be used for our discrediting?

- All confidential communication you have to take over phone should be realised through *Signal* app. Even when you are having a conversation through this app, make sure it is not inside the room you suspect is bugged. Also, it is desirable that you turn on timer for self-destruction of messages after a period of time on the encrypted communication app.

- You must lock your phone with a password. Although there are options for unlocking your phone with facial recognition, fingerprint, typing in pin code or making pattern, the most reliable way of locking phone is installing complex password which contains letters, numbers and symbols.

- Even though your phone is locked with a password, do not leave it unsupervised for a longer period of time and do not take it to service store before you delete all important information from it.

- Make sure that the phone you are not using, and want to give away or sell, is restored to factory settings, meaning you have deleted all data from it. If not necessary, do not give your old phone to others.

Secret surveillance (bugging) of the office

Bugging offices as a form of threatening the confidentiality of information is usually implemented by government institutions, but with the development of technology and more accessible means for bugging this could be done by private agencies, even individuals too.

The ultimate goal of attackers to bug your office is more or less the same as with phone tapping – gathering information on your business activities, gathering information on your working habits and business contacts.

There are not many cases where the bugging devices are detected afterwards, as the procedure of detecting these devices is very expensive and unreliable. It is therefore necessary to focus on prevention.

Attacker's office surveillance requires great resources, so it is not that evident how many organisations and individuals are the object of secret surveillance. Investigative portals desks, as well as the organisations targeted as "enemies" in politicians' statements should have reasonable doubt that their offices are targets of secret surveillance.
We will list potential attacks that are not probable for all types of organisations, so in that sense you have to measure the level of attention you will pay to this threat (the same goes for secret surveillance).

The offices could be bugged in several ways:

- **Installing bugging devices in the office walls**. This should take a lot of time and the government telecommunication infrastructure would be used, so the government authorities will most likely use this type of bugging. For your office to be bugged, it is necessary to have physical access to your office, but the bugging device could be installed into the walls of neighbouring apartments (apartment next door, above or below yours). It is very hard to detect these devices since it is necessary to scan

the walls by special devices, and only specialised agencies can do that and it is quite expensive.
- **Installing portable bugging devices** in furniture or other equipment such as computer, printer, air conditioning and other. Unlike the previous, portable devices require power source (therefore would be usually installed into other electrical devices) and have to use some type of signal for the communication with the attacker (radio, GSM and Internet), so it is easier to detect them. These devices could be more dangerous compared to fixed devices because they require less time to be installed and could be planted to you when you are buying the equipment.
- **Abuse of existing resources for bugging the office** requires physical or software adjustment of electrical devices which already have necessary parts for audio recordings. Devices that could be physically adjusted into bugging devices are landline phones and intercoms. When installing virus into a mobile phone or computer they could be transformed into a bugging device.
- **Remote office bugging** is implemented with directional microphones if necessary and it could be performed from the office in the building across. Some versions of directional microphones can be installed as an accessory to a phone, which could be used for bugging your meetings in the public place.
- **Video-surveillance of the office or office entrance** is also an option for attackers to use, particularly if they want to know who comes to your office or if they want to monitor your movement and thus facilitate the tailing later on. The attackers can secretly record your office and its entrance into several ways:

  - **Installing fixed cameras near the entrance to your office** – these could be visible, but you will not know who the user is, and they could be hidden – in particular if they are right next to the entrance of your office; for this purpose government actors may use public cameras used by the police;
  - **Recording by phone or portable cameras** – the attackers may do this if necessary, within the scope of their tailing actions;
  - **Installing hidden cameras inside the office** – especially inconvenient since it could be combined with bugging the office;
  - **Abusing your system of video surveillance –** this is more probable action for attacker, if you have an option of remotely accessing the cameras; in this case the attacker might access your account for watching the security cameras videos, even the archived recordings.

Useful advice on how to prevent and, more rarely, remove the secret surveillance devices:

- Conduct all confidential conversations outside the office, and do not agree on time and place of the important meeting in the office.

- Avoid meeting confidential sources in your office.

- Efficient and cheap method of preventing secret eavesdropping could be playing loud music or other loud sounds while you speak in quiet tone.

- When finding new office space keep in mind who occupied the premises before you – avoid premises which might have been occupied by potential targets of secret surveillance.

- Do not publish your new address until you move into the new premises and set up the security system.

- When procuring electrical devices, including fridge, microwave, air-conditioning and other, computer and phones too, avoid phone orders and always try to buy it in person.

- Fixing the electrical devices, delegate it to electricians you know personally, but do not leave electrical devices in their workshops without supervision.

- By using relatively cheap device for detecting secret cameras (about EUR 15) you can detect and remove hidden cameras. Hidden cameras are usually set in the cracks (holes) of other devices, so by using these devices try to find lenses inside the socket or air vent. Unlike the secret eavesdropping of the office, you can definitely find the hidden camera if you are persistent and know where to look.

- You have to take seriously the password for remote access to video surveillance system because if they break the password the attackers will possess the surveillance over your office, as well as the access to video archive of your recordings. It would be the best if only one or two persons in the office would have the password and they should give access and create usernames for other users to access the application for monitoring the surveillance.

Unauthorised access to email and social media accounts

Danger of hacking your email and social media account has several aspects. In addition to unauthorised access to information, there is danger of deleting data, and abuse of your accounts for false representation and disseminating disinformation.

Attackers may implement this kind of activity as a “revenge” for some of our activities, but also as regular sabotage of our activities.

In this case the attackers must have special knowledge and skills and they do not have to be a part of some group of typical attackers (right-wing groups). Usually this attacker would be some fanatical individual in need of praise, a hired attacker or a member of secret service.

There are several potential scenarios:

- Hacking email accounts and social media accounts so we will not even notice. The goal of these attacks is most often only to get information from these accounts, and it could be also to use our accounts for disseminating disinformation by sending emails or messages to other users. If this attack happens to some of the activists’ private accounts, the goal might be to gather discrediting information.
- Hacking email account and social media account with primary aim of occupying our accounts. In this case the attackers will change the password and disable legitimate moderators to access the accounts. In this case, it might happen that for some time the attacker will disseminate disinformation by pretending to be a legitimate moderator. It might be that they will also post their symbols or insulting comments (on social media), it happens when attacker wants to “demonstrate strength”, making a clear point to everyone they have managed to access your accounts.
- Hacking email account and social media account with the aim to destroy all data found in them.

The following advice might help you prevent such account attacks or minimise the damage caused:

- You must have strong password. Strong password rules are the following (to be applied when making any kind of password):
  - Password must have minimum 16 characters, but it is good if it is longer.
  - Password must have uppercase letters, lowercase letters, numbers and symbols.
  - Password must not contain dictionary words (or should have as few as possible, in combination with other characters).
  - It would be good not to use obvious, common *leetspeak*, e.g. substituting letter O with 0, or letter A with 4.
  - Password should not contain any of your personal data – date of birth, phone number and other.
  - Don’t use series of same letter in a password, such as “hhhhhhhhh”.

- Do not use the same password for several accounts.

- Store your password safely – in *Keepass* app and do not write it down.

- Change your password periodically – at least every couple of months, preferably every 15 days.

- If several persons use the same account, distribute the new password through *Signal* app.

- Limit the account access to essential number of people. It is not necessary that all members of the organisation have access to email account and social media accounts.

- Whenever possible, “two steps verification” should be set up for all accounts.

- Pay additional attention to the possibility of stealing password by the means of social engineering (read about it in a special chapter).

- Never communicate with your confidential source, or take any kind of confidential communication through email (unless it is encrypted) or social media.

- With all your important partners, activists, sources or persons with whom it is important to maintain communication, you should have at least two communication channels, so you should not rely on email and Facebook communication only, but must have their phone number or another email address.

- If your email and social media accounts were hacked, you must announce that on your official website.

- The first thing to do after attack is to address the administration in charge of your account (*Google*, *Facebook*, *Twitter* and other).

- If you have lost access to email account and social media accounts due to hacking, you have to inform your partners and donors about it individually and tell them that you do not have the control over those accounts anymore so if they receive any messages coming from those accounts that these are not from you.

- Report the attack to the police.

DDoS attacks

DDoS attack is the attacker's attempt to make your website inaccessible to users. Attackers will disable the computer, network or some other part of infrastructure to prevent users from using it. In addition to websites, the DDoS attacks targets could be our web and file servers, as well as applications and other online platforms.

Unlike other attacks that we have mentioned before, here in addition to standard attackers we have several other categories such as – **hacktivists**, i.e. fanatic individuals who see the attack as a form of political expression; **vandals**, who will bring down the site because of their obnoxiousness or to show off; **blackmailers**, who will ask for money to stop the attack or not to launch it. The most probable attackers will probably be the **hired attackers**, who can get orders from all attackers previously mentioned – politicians, interest groups and extreme organisations.

Majority of attacks will last only one day, and NGO and media organisation websites mostly are not of commercial type, so there will be no material damage or it will be insignificant. The real damage will be that our readers and fans will not be able to access our website content. Media organisations will suffer the greatest damage, as their success depends on the readers being able to timely access the news.

In order to respond to DDoS and mitigate the risk of its occurrence, we need experts, but we should keep in mind several other useful things:

- **Believe that DdoS** attack will happen – This attack does not require too much resources (it will cost 10$ to 1000$ per attack per day) and it is often performed, and is especially beneficial when the attackers want to stop the line of communication between the audience and the few free media sources in Serbia. In that sense, it is obligatory to make detailed procedures in the event of an attack, with obligatory information for your team IT expert or temporarily hired IT. The procedure should also include your Internet provider contact, as well as a list of questions to ask.

- **Take preventive measures to protect from DDoS attack** – first of all, by making the lists of launched server processes (and the list of network connections for services), then disabling of the process, except those required for server to function normally and in the end filtering packets. The goal of packets filtering is to disable attackers to fake their IP address, and to block packets coming from unknowns addresses and ensure the supervision over services.

- **Website should be distributed through multiple servers –** so in case of a DdoS attack on one server, the website would be available from another server. This is the most efficient retroactive action in case of the DdoS attack.

- **Use service for attack mitigation –** majority providers of this type of service offer 7-day trial period, and then you have to pay the subscription, while some providers, such as *CloudFlare*, offer the basic service package free of charge.

- **Good communication strategy** to be developed for alternative communication with your audience in the event of an attack – this involves the protocol of sending notifications to mailing list prepared in advance, sending information through your organisation social media account or with the help of partner organisations.

Social engineering

Social engineering is a type of attack that relies on manipulation, whereas the attacker fraudulently forces employees to violate security procedures. The ultimate goal of an attack can be to steal information, equipment or money. In investigative journalism, attackers use social engineering to get information about sources or stories we work on, but also to provide for themselves access to the office (and subsequently open up the possibility of bugging offices or conducting a secret search).

Three basic groups of social engineering techniques are impersonation, using the victim's lack of attention and the technique of reverse social engineering.

When it comes to the first group of techniques, the attacker impersonates either **as an employee from your organisation** if your organisation is large (as someone with a higher position, someone from another office – editorial team from another city, a new employee who needs help, an employee in the IT sector), or as **an employee from another organisation** (employed by a partner organisation, tax inspector, employee of a company that commonly provides services to you, etc.). The best way to counter this type of social engineering is to establish procedures and strictly adhere to them – such as the procedure for receiving uninvited guests, the procedure for arranging contracting with companies that provide services for us, the procedure for answering the phone, etc.

Using a victim's lack of attention involves several different techniques:

- eavesdropping in public
- "shoulder surfing" – when we type a password or a PIN code
- secret search of an office
- secret search of one's computer
- "holding doors for someone" – when the attacker takes advantage of a victim by "holding the door politely" as they enter the building and the attacker thus enters without a key
- searching through one's waste – documents not properly destroyed

- installing malware – when the attacker has physical access to a computer or phone
- setting up a key logger – a piece of equipment that is fixed to a keyboard or USB inputs that is unnoticeable and collects data for an attacker
- "phishing" – when an attacker sends you a fake website (which looks like a legitimate site, such as a G-mail or bank you use) to fraudulently take your personal information.

The reverse social engineering technique involves several steps to make attacker's fraud more compelling.

The first step is sabotage. For instance, the attacker will arrange for you to lose Internet access.

The second step is to promote the attacker. The attacker will call you and impersonate your Internet service provider to ask you if you have Internet access "because they have detected interference in your neighbourhood" and he will say that he will send a team to check your modem.

The third step is to "assist" the victim. "The Internet service provider team" will come and bring in a new, "correct" router, which is wiretapped or allows the attacker to monitor your Internet communication.

There are several other ways to recognize social engineering. Pay extra attention in the following situations:

1. When you receive any kind of request from a stranger that sounds common but it is contrary to your procedures (especially security related ones)
2. A direct question during the conversation regarding information you consider to be a secret
3. Excessive interest in information that is public, but related to employees (how many employees there are, who performs which tasks, etc.)
4. Too long a conversation on a non-business related topic (if you only have a business relationship with that person)
5. Flattery
6. Presenting something as an emergency
7. A person presents himself/herself as someone in a high position. ("loud boasting", "Do you know who I am?")
8. Covert or direct threat
9. "Marketing Research" – phone calls where the attacker, under the guise of a market researcher, makes inquiries about various details.

Theft of documents, information and data carriers

Targeted document or data carrier theft (USB, laptops, phones, etc.) can be directed primarily towards investigative journalists, but also towards activists who are the targets of secret services.

The attackers could be the persons we are investigating or someone hired by them as well as secret services – if we are talking about investigative journalists. In the case of NGOs, these will most often be members of the secret services.

The damage that can be caused is not just that someone will gain unauthorized access to information and find out something that we considered to be confidential or secret information, but that if we did not have a backup of the information, we would lose it.

How is the theft of documents, information and data carriers performed?

- **Burglary into the apartment or office** where the documents or any device on which the data can be stored are located. To conceal the right intention, burglars can fake burglary to steal money, jewellery or technical equipment. It is possible that someone will steal only the necessary documents, but this will immediately point to a possible profile of the attacker.
- **Copying documents during a secret search of an apartment, office or hotel room** is an even more probable situation, since, if skilfully executed, it leaves no evidence that anything has been copied. Physical documentation can be photographed and information stored on computers, phones and external disks can be copied. Performing such an action is much more complicated than a simple burglary, but the assumption is that it happens more often.
- **Breaking into a car** where we left our documents can happen especially if someone has previously observed our movements and habits.
- **Forcible seizure of documents or data carriers in the field –** someone with the threat of violence can seize our backpack with documents, laptop or phone or simply rip it out of our hand.
- **Theft in the field / pickpocketing** is also an option – with our negligence, someone can steal our phone or documents or laptop from our backpack.

What we can do to prevent or minimize damage?

- At the organisation level, we will establish clear and strict document - specific procedures. Procedures must include rules for keeping, using and carrying documentation.
- All information we work with must be classified into public, confidential and secret (this will be discussed further in the guidelines) and then we will apply different procedures to them, depending exactly on how we classified them.
- We will keep the documentation and data carriers that we have marked as secret in a safe or locked file cabinet at all times when we do not use them.
- We will keep the documentation we have marked as confidential in a locked cabinet or in a part of the office that is locked outside working hours.
- We will stick to the clean table policy, i.e. at the end of working hours we will inspect the table and make sure that there is nothing left of the documentation that we have determined to be secret or confidential. Also, we will make sure that none of the documentation we have classified as confidential or secret is exposed on the desk when we have visitors.
- All media should be encrypted.
- We will not take any documents that we have marked confidential or secret out of the office, except in exceptional circumstances, and on such an occasion we will keep it by our side all the time.
- We need to have backups of the documentation (at least the one we marked as confidential or secret) and we will keep those copies, like the original, in the manner provided for the degree of their secrecy.
- Hotel room, apartment or office – all the places that can be subject to a secret search can be secured by a motion activated camera. The solutions may be a "baby camera", which is cheaper, but is visible and dependent on electricity and the Internet, or a hidden camera, which is slightly more expensive but imperceptible and is most often independent of energy sources and the Internet (the footage is reviewed afterwards).
- We will never enter secret journalistic sources in the phone book under their real name and we will regularly delete all communication with them from the phone.
- The phone will be protected by a password – the most preferred password is a

combination of letters, numbers and characters.

CAMPAIGNS AGAINST NGOS AND JOURNALISTS

Campaigns against NGOs and journalists can be conducted by all sources of threats – primarily by officials, political parties, pro-government media, but also by various interest groups. The campaigns are run through statements by officials, media campaigns and social media campaigns.

The main consequences of such campaigns, regardless of who conducts them, are: targeting activists and journalists as legitimate targets for further attacks of all kinds, reducing public support and preoccupation of the organisation with topics that are not of primary importance to them, and may result in a decline in activists' and journalists' morale and the rejection of possible sympathizers.

We have to take campaigns against our organisations or individuals from organisations with utter seriousness, because examples so far have shown that campaigns are often the precursor to assaults.

Campaigns conducted through statements of the officials have the most impact on the general public. Officials have the support of their party colleagues, sympathizers of their political option, the media in their favour, as well as social media bots – so this campaign, in fact, continues through the media and social media. Campaigns can consist of distortion of the facts, spreading misinformation, disparaging the work of organisations, and even openly insulting activists and journalists. A special type of negative campaigning by officials is unfounded accusations against NGOs and journalists.

Media campaigns do not necessarily have to be accompanied by statements made by officials, but they also have a strong impact on the public and send a clear message to our organisations provided that we know whom particular media generally supports. These campaigns, similar to campaigns run through officials' statements may consist of distortion of the facts and spreading misinformation, but may be substantiated by statements made by "experts" or "anonymous sources" and thus have more capacity to produce more complex constructions and spins when compared to the statements of the officials.

Campaigns run on social media tend to boil down to open insults and threats to the organisation, activists and journalists. They aim to send a bad image of the organisation to the public, scare activists and journalists, and reject sympathizers. Such attacks often seem to be attacks by a number of individuals, but there is every chance that these are made by organized groups of Internet activists working at the behest of political and interest groups.

What can we do, what is at our disposal to minimize the damage from campaigns like this?

Reporting attacks from our point of view is a key point in countering negative campaigns. In the case of campaigns run by officials, in our reporting we will point out all possible violations of the law, incorrect behaviour of officials, and their supposed ultimate intent. In the case of media spins, in addition to informing the public ourselves of the intent of the media involved in the attack, we will also report the case to the media involved in the analysis of fake news. We will certainly report on social media campaigns when it comes to an open threat, while in the case of negative comments and insults there is no great need for reporting. We will also ask all partner organisations for assistance in reporting.

Addressing international institutions and organisations is essential, first of all, because of the extreme statements of officials and any calls for violence. After the institution or organisation condemns the campaign, it would be a good idea to share the news.

The gathering of evidence is crucial for reporting what happened to the police, for possible private lawsuits, but also for invalidating possible campaigners' denials. In this way, we will collect videos, copies of print editions, and take screenshots of all the statements we have identified as parts of the negative campaign.

Hiring a lawyer, first and foremost, to distinguish threats from insults and thus to know what to report to the police. Secondly, we will also hire a lawyer to file a lawsuit against authors of negative media campaigns.

Reporting to the police all comments and statements on social media for which our lawyer confirmed to us to be having grounds for reporting**.**

Creating an internal database of all negative campaigns and threats will help us anticipate future events, better report them, but also alert partner organisations if we decide not to report on some campaigns.

Investigating the goals and background of the campaign – an attempt to understand the background to the whole attack, especially if there were multiple texts, and put them in a broader context to understand how they came about, who was behind them and what triggered the reaction. This will be of particular help to us in the future to anticipate the attacks and better prepare ourselves for the response.

HOW DO WE FIGHT BACK?

In this chapter, regardless of the types of threats that may be posed, we will list helpful tips for the safety of the organisation and individuals. Acceptance of these tips will contribute to raising the level of safety culture, which is the ultimate goal of developing a safety system.

IMPORTANCE OF BEING INFORMED (ABOUT THE ATTACKER, THE IMPORTANCE OF THE THREAT, THE EXPERIENCES OF OTHER ORGANISATIONS)

As we noted at the beginning, the main problem regarding safety in NGOs in Serbia is the lack of a systematic approach, while the advantage is good communication and exchange of experience between organisations.

The main prerequisite for a systematic approach is being well informed on possible attackers and threats, which, given good communication between NGOs, should not be a problem.

Being informed about possible attackers gives us an idea of when and what kind of attack we can expect and it will also make it easier for us to subsequently identify the attacker as we have already narrowed a list of suspects.

The best way to systematically collect information about attackers is to make an internal note after each incident about what happened. So over time we will create a database of all the attackers, from where we can see what kind of attacks these attackers are prone to, who their accomplices may be, and when we can expect an attack from each of them. This kind of information is crucial for the development of a safety system within an organisation. Such databases are even more useful when they are set up and systematically supplemented at the level of several like-minded organisations.

In addition, it would be a good idea to keep track of news, announcements and scientific papers related to the attackers. It is important to be informed, in general, of the ideology and "moral values" of the attacker, as well as of specific organisations and individuals.

An even more important thing about safety is **being well informed about what forms of threats are occurring and to what extent each of them is dangerous to us**. This apparently seems easy to assume, but does require a more detailed analysis. A good example is a secret following, behind which can be hidden a dozen different targets of the attacker – from routinely recording your habits to preparing for kidnapping or murder.

That is why it is important that we educate ourselves on all possible threats and try to understand all the mechanisms of how the threats come about. In addition to the ways of being informed we have mentioned when talking about being informed about potential attackers, seminars on the topic of safety, as well as courses that counter this particular type of threat, may be more helpful.

Also, research and texts published by foreign or international organisations may be useful, since, unlike information on specific attackers, information on the forms of threats and their consequences is largely universal – valid in all countries. In order to understand the particularities that depend on the country in which you work, it is important to have a better understanding of the socio-political situation.

As we said, for being well informed on attackers and threats, **good communication with like-minded organisations** is crucial, first and foremost for sharing experiences. Knowing this, we need to organize as many roundtables, seminars and joint workshops as possible on the topic of safety. It is especially helpful to establish and maintain shared databases concerning attacks and attackers.

PERSONAL SAFETY AND SELF-DEFENCE

The issue of personal safety should be open-ended for everyone, no matter what their business is. Given that NGO activists and journalists in Serbia are often targeted by various attacks, including assaults, personal safety needs to be given more attention.

There are a few major rules when it comes to personal safety, no matter what type of attack it is.

1. **Awareness of the environment** is a key factor, above all, in order to recognize the threat in a timely manner. Here we are talking about the ability to notice the person who stands out from the environment, to know at any time which familiar object is located nearby, where the nearest taxi station might be, etc. Although at first glance, it seems exhausting, it is just a concentration that we can easily direct to the right thing – provided that while we are walking down the street, we are not looking at the phone or listening to music.

2. **Find out as much as you can about the place you are in,** and especially about the premises you often spend your time in – the buildings you live in and where you work. First of all, this means that we know at all times where the exit from the room and from the facility is – which is vital to us when we have to leave that place quickly. In addition to the main entrance/exit, we must also pay attention to alternative exits from the room, as well as furniture and items in the room, as some of these can be used for shelter and some as a convenient weapon for self-defence.

3. **Listen to your instinct,** because instinct is not something abstract, but the sum of a multitude of signals that want to alert us to something. It is not necessary to panic or abruptly react, but be sure to take instinct into account when deciding what your next action will be, and especially when considering whether or not a situation is dangerous.

4. **Have a plan,** i.e. think about dangerous situations beforehand. For each of the assumed situations, think of how you will respond, where you will escape, what will be your first action after the incident is over. Although we assume that we will respond instinctively in crisis situations, it is, in fact, most often the result of some of our earlier planning.

5. **Report everything that is suspicious.** Most serious threats to personal safety are preceded by some kind of warning or prepping action that we may notice. If suspicious actions are noticed on time, we will report them to the editor, director or our immediate supervisor, and, if necessary, to the police. Reporting suspicious events will certainly help your organisation take the necessary steps to protect you, and your view that you are aware of the danger and the fact that you have notified other people will repel the attackers. In the worst-case scenario, reporting suspicious events and persons will later, after the attack, make it easier to identify the attacker.

Here are some more helpful personal safety tips:

- Always be prepared to confront in any available way. Never get accustomed to the role of a victim.

- When you notice suspicious persons, i.e. possible attackers, keep your distance from them, but if you still come close to them, with some excuse, raise your hands to chest height or higher (adjusting your hair, holding your lapels, etc.) – this will shorten the time of your reaction to the attack (blocking or hitting back). If the person is addressing you in a threatening tone, address him calmly with your arms raised at chest height and palms facing him.
- If physical confrontation occurs, make sure you stay on your feet at all costs. Falling to the ground greatly reduces your chance of defending yourself.
- If you are attacked in an elevator, do not press the alarm button – this will stop the elevator. Press the button for the first next floor.
- If the attacker asks you only for money, throw your wallet a few meters away from the attacker and use that moment to escape.
- If you have young children, teach them to hide behind you upon the agreed sign. You do not have to scare them; you can teach them this while playing.
- If you have already got into a car where the driver seems suspicious, call someone you are close to by phone and mention in a chat what kind of car you are driving in (make and colour), where you got in the car and where you are up to – you will do this so that the driver hears everything. It is also a good habit to remember the license plate number and write it in your phone before you get in the car.

OFFICE SECURITY

Physical security of the office

It is important to focus on office security because we are also improving all other aspects of security – personal safety, data and equipment security. We will list all aspects of office security, but the choice of them depends mostly on the budget allocated for security, the threats to your organisation, and the characteristics of your organisation.

Security door should be installed if there is a risk of vandalism, theft of equipment or physical attack on the office**.**

Security locks are far more important to protect the newspaper office because those involved in investigative journalism are at high risk of secret entry and search of the office. Security locks will prevent the attacker from entering the office without visible traces. Good security locks include new generation keys whose prints cannot be taken and cannot be copied without a special card. Like security software, new generation locks appear periodically.

Window security bars are required if your office is at ground floor. The bars do not

provide protection against vandalism (breaking windows), but do provide protection against possible burglary.

Safes play an important role in protecting data as well as equipment. The important thing is that they do not have electronic parts (especially not the code to be entered, instead of the standard key), to be large enough for your laptop to fit inside, to be screwed into the pad and placed in a hidden place. Ideally, safes will be located in a corner of the room, screwed into the floor (not in furniture), and "masked" by furniture.

Alarm system is the most important part of securing an office. Its task is to register incidents and notify alarm users thereof. Illegal entry into the office outside working hours is recorded by motion detectors and magnetic contacts, which are placed at all possible entrances to the office. Part of the alarm system can also be fire detectors, as well as a "silent alert" (a button that soundlessly activates and reports to someone outside the office that an incident has occurred). The siren is also part of the alarm and has the role of causing the attacker to panic and inform people in the surrounding area that an incident has occurred. It is important for the alarm system to have a backup battery, alert users via the GSM network (SMS) and be programmed so that each user has his or her password and account on the alarm (unless the organisation is too large).

Security cameras are a complement to the alarm system, but are used independently. The cameras can be visible or hidden, with or without night vision recording, with or without integrated memory and the ability to track the video over the Internet. Cameras should be placed on the outside of all potential office entrances, and it is best to select visible night vision cameras. If your budget is limited, you may consider setting up fake cameras to help deter potential attackers from attacking. The security camera recorder (the part of the system that stores the footage and allows online tracking of the footage) should be hidden inside the office, secured and with an extra battery and able to store the footage for at least two weeks. If you choose the option of keeping track of your recordings or keeping copies of them online, make sure you create a strong password to access the applications that allow you to do so.

Access control and detection system helps us control identification, enable selective access, and keep track of how long someone has stayed in the office. Unlike alarms, we use this system during working hours. We need this if the organisation is large and the frequency of use of the front door is high. In this case, employees receive tokens or cards that unlock the front door during working hours. If the cards are personalized, then the system can keep track of who used the card, and so hours can be recorded.

Preferred security procedures (examples)

All of our work (both of individuals and organisations), and in particular working together in the office, should be defined by clear security procedures. Regardless of the money invested in the security system, it does not mean much without clearly defined procedures and their consistent implementation. By disciplined and persistent implementing procedures at the level of the organisation, but at an individual level as well, we develop a safety culture – which is our main goal.

Security procedures are compiled for all most common situations we might find in our work. We prescribe them based on our experiences, the experiences of similar organisations, but mostly based on the knowledge we have gained about security tools, possible attacks and attackers.

These procedures can be printed in text or displayed in algorithms. They must be accessible to anyone whose work they relate to, but will remain marked as confidential, i.e. will not be available to the public.

The examples of security procedures (they are not recommended for all organisations, but represent just an example):

1. **The procedure of receiving guests** is a basic and everyday procedure that must exist in all organisations.

- We do not welcome guests in the office who have not been previously announced.
- If a guest appears at the door claiming to have previously announced himself, we will ask him to wait outside the door until we check that. If we do not manage to determine this, we will ask him for his contact details and say we will get back to him.
- We do not accept people in the office who want to promote a product or sell some services, regardless of the fact that they have previously tried to announce themselves.
- When the guest announces himself in advance, we will take his contact details, record the date, time and the name of the person he wants to meet. We will pass this on to a colleague who is expecting a visitor, and we will tell the guest that a colleague will contact him to confirm his visit.
- Immediately before the guest arrives, we will designate a meeting room.
- We will review the room in which we will have a meeting and see if any document that has been marked as secret may be exposed.
- During the visit we will discreetly control the movement of the guest so that he does not enter other rooms at his discretion.
- If the visitor turns out to be aggressive or suspicious on any other grounds, we will save a recording of his visit (from our security cameras) and review it in detail.

2. **The procedure of organizing events in our space** is necessary for those organisations that have the capacity to organize events in their space. It is even more of a challenge if we give away our space to other event organisations.

- We have a list of entities to which we will not rent our space.
- If an organisation with which we have not previously cooperated comes forward, we will first check if there were incidents at their events.
- Before we finally arrange an event, we will collect information from the organizer about the topic of the event, whether the event is open or closed, the number of participants, as well as the expected threats.
- We will then decide whether to rent the space.
- We will remind the organizer to contact the police if the event is risky.
- During the event, as necessary, we will provide the organizer with the necessary support related to security – we will hire a security guards that we normally hire, record the event, etc.
- If an incident occurs, we will provide all available support to the organizer.

3. **The procedure of leaving** the office involves several actions of checking the workspace and setting up the alarm system.

- At the end of working hours, we will check if we have shut down our computer and then store it in a safe place (safe, safety cabinet or locked drawer).
- All documents used throughout the day will be returned to their place and provided in accordance with the *Static Information Protection Plan*.
- We will double-check the desk to see if any documents are left on it.

- We will close the windows in our part of the office.
- If we are the last one who leaves the office, we will check that windows are closed in all parts of the office.
- We will lock the door of our part of the office.
- If we are the last one who leaves the office, we will set up the alarm system and lock all the locks on the front door.

4. **Procedure for reporting threats on social media** should also exist in all organisations that face threats.

- If we notice an offensive or threatening comment on social media, we will take a screenshot of that comment and save it in the folder previously provided for it.
- We will delete a comment from our account.
- We will then notify other employees of that comment.
- In consultation with everyone in the organisation, we decide whether it is a threat or an insult.
- If it is a threat, we will report the case to the police.
- After reporting the case to the police, we will decide whether or not to make a statement about it at the organisation level.

SECURITY OF INFORMATION

Before mentioning specific tools, we need to classify all the information at our disposal and assign them a degree of secrecy. Besides, we will distinguish between static and dynamic information. Static information is information we store and work with, and dynamic information is information exchanged within the organisation or with partners.

Classification of information

Public information makes up most of the information and documents we work with. This is all information and documents that cannot be misused in the negative campaigns and sabotage of our actions.

For example, these may be documents obtained under the Law on Free Access to Information of Public Importance, or documents from different archives, on the basis of which we have written some of our publications.

Such information and documents will not necessarily be disclosed to the public, but will not be strictly controlled by who can access them.

Confidential information can be a big part of the documentation we work with, but it depends on the type of our organisation – if we are the editorial board of a research portal, we will work with slightly more confidential information than an NGO dealing with the national minority rights.

Confidential information is information whose disclosure is not critical to the security of the organisation and activists, but when used in a specific context they can be used against us. These may be contracts of employment, financial documentation, projects we have prepared for donors, as well as information on specific topics that we will address in the coming period.

We will keep confidential information in a more cautious manner than public information – we will restrict access to this information within the organisation, it will be stored in a part of the office that is being locked and we will not keep it on an unsecured server.

There is significantly less **secret information** when compared to public and confidential information, but we must pay the utmost attention to its safekeeping and sharing. It is information whose disclosure may directly endanger the security of the organisation, activists, journalistic sources, NGO users or any other person.

The example of secret information could be personal information of the user of an NGO dealing with the protection of human rights (especially victims of violence), information about a secret journalistic source, documentation obtained from a secret source, the text of the research story before it was published and passwords for all the accounts used by the organisation or activists.

We will keep secret information with much more care than any other information. The information we store will be stored in encrypted files (if they are in electronic form), or in a safe in the office (in the case of physical documentation). If we exchange them, we send them via the Signal app if we send them over the phone or via encrypted email, if we do it via computer.

Plans for information storage

Once we have classified the information in this way, we will make a plan for storing i.e. protecting it. Two separate plans need to be made – one for the information we store and one for the information we exchange. Both plans take the form of a table.

The static information protection plan should first and foremost contain all the information we store, whether it is data in physical or electronic form (we will also emphasize the form). We will then determine for each piece of information listed where it will be stored, e.g. "in the closet in the programme director's office." We will then limit the information to a specific circle of users, e.g. "financial management". Then we will mark the information by degree of secrecy. Finally, we will outline a specific tool or technique to help protect that information, e.g. "We keep the documents in an encrypted folder" or "We keep the documents in a safe."

STATIC INFORMATION				
INFORMATION CHARACTERISTICS				
WHICH INFORMATION?	WHERE ARE WE STORING THE INFORMATION?	WHO SHOULD HAVE ACCESS TO INFORMATION?	HOW SENSITIVE IS THE INFORMATION?	WHAT IS THE MEASURE OF PROTECTION?
Financial documentation in electronic form.	In financial manager laptop. Backed up on the external hard disk.	Management	Confidential information	Stored in encrypted folder. Daily back up in separate external encrypted hard disk. Laptop and hard disk kept in separate safe boxes.

A dynamic information protection plan refers to protecting all information that we exchange, either internally or with someone outside the organisation. Again, we will first state what information is involved, e.g. "emails exchanged between team members containing survey details". Then we will specify the method of information exchange – in this case it could be Gmail. We will also indicate who will have access to this information, so, for example, we will say

for these emails that they can be accessed by "team members exchanging emails and Internet service provider". We will then list all the physical and virtual channels that the information occupies, e.g. "Source: team member computers, path: Internet – via Google services, target: team member computers." We will mark the information with a degree of secrecy and finally determine the method of protection for it, e.g. GPG encryption.

INFORMATIONS IN MOTION					
MENAGING SOCIAL NETWORKS					
WHICH INFORMATION?	WHERE ARE WE STORING THE INFORMATION?	WHO SHOULD HAVE ACCESS TO INFORMATION?	HOW SENSITIVE IS THE INFORMATION?	WHAT IS THE MEASURE OF PROTECTION?	WHAT IS THE MEASURE OF PROTECTION?
Emails between team members	Email (Gmail)	Team members, email provider	Source: team members' computers Route: Internet (via Google servers) Destination: team members' computers	Confidential information	GPG encryption (Mailvelope)

We will make both documents available to all members of the team, but will not make them publicly available, i.e. we will treat them like other written procedures – as confidential documents.

Mobile phones

Signal Private Messenger is an application that is used for secure communication. Communication is encrypted and cannot be intercepted. The application is specific to a phone number, but it is also possible to connect that account to a computer. The Signal has the same functions as Viber, so it is possible to talk, send messages and files. Installation is quite simple.

1. Download the Signal Private Messenger app from your phone's Play Store.
2. Launch the application and enter your phone number. Once the application identifies that you are using a phone with that phone number, you will be able to access it.
3. The application will search your directory and in Signal you will be able to see all your contacts who use this application.
4. If you also want to connect your Signal account to your computer, you need to download the application from the link https://signal.org/download/ and follow the instructions for connecting.

The application offers the ability to automatically delete messages (you choose the time interval after which the messages will be deleted), which provides additional protection – because the content you sent after a while no longer exists, so you do not leave a trace of communication. The advantage of the application is that there is an option to disable the print screen while in the application.

* Please note that this application will not help you much if you are talking loudly in a room that is bugged, so it is always better to rely on messages.

Computers

Mailvelope is an application we use to encrypt emails. Mailvelope functions with a key split up in two parts. To send an encrypted email to someone, you need to have that person's public key; that person needs to have your public key as well. You can give a public key to anyone. The most important one is a private key, which you will use every time you encrypt or decrypt email – this is a password that you need to think carefully about and keep. Mailvelope is actually an extension for Google Chrome and Firefox, and is linked to your Gmail accounts. Using Mailvelope is not complicated; you need to follow these steps:

1. Download the Mailvelope app from the Chrome Web Store or Firefox Add-ons, after which a padlock and key icon will appear on your browser.
2. When you enter the application, the first thing you need to do is generate your keys – you do this by clicking on "Key management" and then "Generate Key" – there you will enter your first and last name, your email address and the password, which must be strong. Such a password implies a minimum of 32 characters including lowercase, uppercase, numbers, and punctuation marks. After that you click "Generate".
3. After generating the key, you will find your key in the "Display Keys" option. When you click on it, select the option "Export" and make sure that the box "Public", not "Private" is enabled at the top of that window. The file you downloaded on this occasion is your public key and send it to anyone you want to exchange encrypted emails with.
4. In order to insert someone's key into your "directory", you need to have that person send you the key first, which you then save to your computer. You will then go to the "Key Management" page in Mailvelope, select the "Import Key" option and then "select a key text file to import". Here you will select the public key that you previously downloaded. After you have exchanged your public keys, you are ready to send an encrypted email.
5. After selecting the person to whom you are sending the email, click on the blank paper and pen icon. This will open a special encryption box for you. If you would like to send an email to several Mailvelope addresses, enter more public keys in the box above. When you have typed the email, click on the "Encrypt" field and you can now send the encrypted email.
6. When you receive the encrypted email, you just need to drag the cursor over the encrypted body of the email and then the envelope icon with the key will appear. After clicking on it, type in the password you came up with once you generated your key and you will decrypt the email.
7. To encrypt the files you send you must first go to the Mailvelope application, select the "Encryption" page and go to the "File Encryption" option. You click the "+ Add" button on the right and select the file you want to encrypt, and then the "Next" button. In the upper window you will select the people for whom you are encrypting files and after each selected name click "Add", and then "Encrypt". You can safely send such an encrypted file.

Make sure that the subject of the email and the name of the encrypted file do not convey the true content of the email, but that they contain some generic term.

For secure conference video and audio calls, it is best to use the Jitsi website (https://jitsi.org/). By clicking the "Try Jitsy meet" button, you can create a new room where you can invite people to a conference call. In order for someone to access the conversation, it is necessary to have a link that was created on that occasion (e.g. https://meet.jit.si/PerfectBadgersBlossomRapidly). Do not send the link via open mail or chat, but use Signal or encrypt the email with Mailvelope. Pay attention if users you did not invite appear during the conversation.

Veracrypt is a programme that allows us to have an encrypted partition or folder on our computer where we will store the most important documents. You need to download a specific

installation file from https://www.veracrypt.fr/en/Downloads.html, depending on which operating system you use. Then follow the installation instructions from this link https://www.howtogeek.com/howto/6169/use-truecrypt-to-secure-your-data/. When you create an encrypted partition on your computer, it is necessary to be large enough for all the files you want to hide. A good password that you will use to lock a partition or folder is also crucial here. Remember that you must not forget your password – if this happens, you will never be able to access the files again and all you can do is delete them.

The basic protection of your computer is the antivirus software. While there are free versions, better protection is provided by those who are to be purchased. Some of them, like Kaspersky, offer the option of encryption, but more secure encryption is the one with Veracrypt. One of the better antivirus software is F-secure. It also offers the ability to use a VPN (virtual private network). VPN allows you to surf more safely as it gives you the ability to change your location – so you can choose the option to, even though you are in Montenegro, leave information on the Internet that you are accessing it from any other country, e.g. from Japan. This way, you avoid, among other things, having someone monitor and analyse what content and pages you visit.

A similar option is offered by TOR, free software that functions like other browsers – Firefox or Chrome. It is easy to use. At https://www.torproject.org/ you have the option to save it to your computer and you can surf completely safely after installation. What TOR does, and what we do not see, is that it is constantly changing provider information and without our intervention shows that we are accessing the Internet from different parts of the world. In other words, TOR is an automatic VPN. Although that is why it is extremely safe, that is what slows it down, so you should have patience when using it.

PREFERRED SKILLS AND KNOWLEDGE

When it comes to security, there are skills and knowledge that we can always develop, regardless of the specific situation.

- **Awareness of the security situation** in the city, country and region will help us anticipate and prevent most of the attacks. This involves, first of all, awareness of the security situation from the perspective of attacks on NGOs, i.e. awareness of all the threats that NGOs and journalists have faced in recent years. It is best to have good communication with similar organisations and keep track of all their announcements related to attacks.

- **Awareness of the activities of right-wing groups, extreme political parties and individuals who are the most common attackers.** The same as being aware of the security situation, a more thorough knowledge of the functioning of these groups will make it easier for us to anticipate their possible attacks. For this reason, we will pay attention to these organisations' public announcements and reports from their events.

- **Awareness of the methods used by the secret services** is also helpful when trying to recognize secret following, secret monitoring, and even when it comes to the understanding of the negative campaigns that can be undertaken against us in the media and on social media. It is not always easy to get informed, but research and studies by NGOs dealing with the topic of the work of security services should be checked.

- **Awareness of legal provisions** regarding our rights and obligations while performing street actions, recognizing and processing threats, as well as copyrights. Knowledge of legal norms will help us know to what extent we can confront in crisis situations without breaking the law.

- **Using encryption software –** of both static and dynamic information. In most cases, using the software is not complicated, but it is good to get to know it in time so that we can use it quickly when need be.

- **Using an alarm and security camera systems** are routine activities, but they require minimal training by employees of the company that provided you with the space or someone from your organisation who is versed in operating these systems. Each employee needs to be taught how to enable and disable the alarm, view and save security camera footage.

- **Self-defence skills** can be crucial in situations of assaults. These skills include the ability of safe falling, running, fighting, and using handy means for self-defence. All of the above skills can be acquired by training some martial arts, where priority should be given to modern, practical skills.

- **Awareness of the functioning of your organisation's website.** In addition to the fact that we need this to maintain the site, knowing its functioning will help us identify the problem that has arisen and which we will further present to the person who maintains it.

- **Awareness of spinning methods and spreading fake news** is crucial for understanding all the problems associated with negative campaigns, whether conducted through the media or social media.

SAFETY CULTURE

A developed safety culture at the level of the organisation is the ultimate goal and the best prevention of all types of attacks. With a developed safety culture, we will be more effective in counteracting attacks, saving the time, energy and resources we truly need to achieve the goals that our organisations exist for.

In our case, safety culture is defined as a set of attitudes, knowledge, skills and rules in the field of safety that we express through our daily behaviour in order to protect the personal values, values of our organisation, as well as universal human values.

It is part of culture in general and it determines our everyday behaviour so that we can more easily identify the dangers, more easily avoid or eliminate them – on our own or by referring to professional organisations.

How is a safety culture created and developed?

Like any other learned behaviour, safety culture cannot be developed overnight, but rather needs to be thoroughly set up, developed and practiced through the persistent repetition of safety procedures.

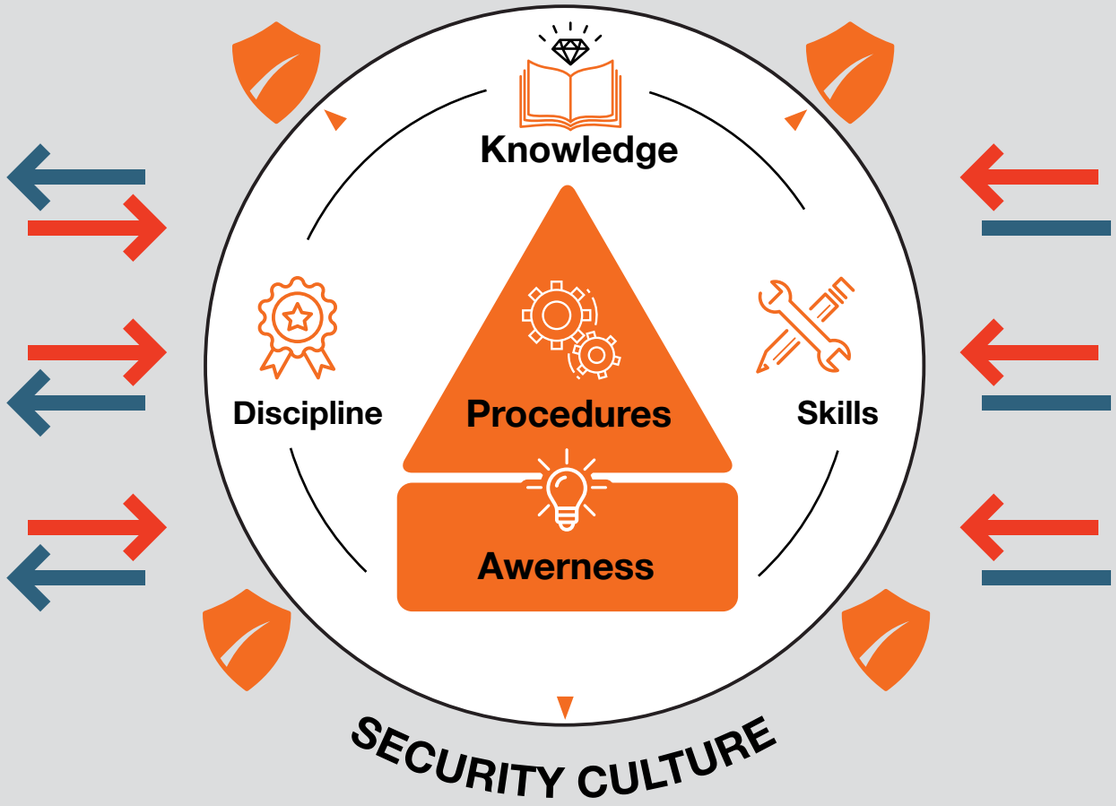
There are four key elements to developing a safety culture for both individuals and organisations:

- **Knowledge –** primarily about security threats, attackers, the functioning of the security systems we use, etc. We must acquire knowledge first and foremost by ourselves: we must be interested in the security issues of our organisation and make an effort to learn as much as possible about security, even when it comes to our personal safety and our role in the security system of the organisation.

- **Skills** as applied knowledge are necessary for us to be effective in counteracting threats. Knowledge without the skills that make it applicable can only be used to teach others to an insufficient extent. These are skills from the previous chapter, but also any application of security procedures that we have adopted as an organisation, whether it be using encryption tools, using a GPS locator or writing reports of the events that we send to the police.

- **Discipline** is an element of a safety culture without which the two previous ones do not mean much. We need to adopt every security procedure we have adopted as an organisation on a personal level and apply it whenever necessary. Discipline may be a key element because it creates habits that are at the heart of the safety culture.

- **Vigilance** is an element that allows us to recognize the threat on time, but also to be able to respond to it even in situations where we do not have security procedures in place. Vigilance makes us think often about safety, so it will also help us improve the knowledge and skills we need more often.



DEVELOPMENT OF SAFETY PLANS

At the end of the process of assessing the security situation and establishing the initial system of the organisation, which we will continue to develop – mostly through education and adaptation to new situations, we will make safety plans.

Safety plans are prepared for each of our most common activities that can be subject to threats. Thus, safety plans can be made for the research process, for managing accounts on social media, or for organizing street actions. Plans are somewhat more detailed than the security procedures, but, unlike the procedures, they are not written for each individual situation, but for our most important and riskiest actions.

The plans include the following elements:

The goal we want to achieve. Instead of naming a specific safety plan, we will name it e.g. "Successfully Performing Field Events".

Identified threats – are all the threats that can negatively affect the achievement of a designated goal. These may be e.g. "assault on activists", "intimidation of activists" or "destruction of equipment".

Prevention Resources and Actions – we will list here all the security procedures as well as any technical means that will help us reduce the chance of a threat being realized. In cases where our goal is to successfully carry out the events on the field, these can be procedures for reporting the event to the police, arranging transportation to the venue and getting to know the place where the event will take place.

Threat Response Resources and Actions – are all the procedures that we will activate in the event of a threat coming true, to stop, avoid or minimize the damage, whether we are talking about the threat response we are undertaking at that moment or that we are about to take in the following period. In this case, it may be leaving the scene and going to our premises, contacting police and lawyers and adding incident details to the internal database. Since we can put a lot of items here, to make the plan practical, we will put them in chronological order.

Emergency Plan – also covers the procedures we resort to after the threat has arisen, but also during its actual realization. We need to know this part of the plan at all times because a written plan will not be available to us when we need to act urgently. This may include trying to calm the situation, joint defence, withdrawal from the scene, etc.

Quality of life plans – are an integral part of a safety plan that describes all the actions we will take to reduce stress and fear of all members of our organisations who have been the immediate and indirect victims of threats. These plans will minimize the long-term damage that would affect the health and morale of the members of the organisation. These may be days off, going out for dinner together, or professional psychological support.

The necessary equipment and information, i.e. all resources that we will use to accomplish any of the mentioned safety plan procedures and actions will be listed in this section. These can be information about the place where we are preparing the event, information about potential attackers, means for self-defence and mobile phones to record the event**.**

We will present safety plans to all members of the team, and in addition we will remind them and share the roles in individual security procedures at the meeting immediately before the action for which the safety plan is intended. As mentioned above, safety plans do not have to be intended for a particular event, but can also be applied to day-to-day or long-term processes and actions that may be compromised.

SAFETY PLANS

GOAL:	Rad na socijalnim mrežama
Threats identified:	• Threats through social media. • Negative campaign on social media against our activists/journalists individually. • Negative campaign on social media against our organisations. • Intimidation of sympathisers via social media before our events • Conscienceless/unprofessional account management on social media. • Unauthorized access to accounts on social media.
Resources and prevention actions:	• Existence of an internal database on social media threats. • Regular reporting of negative campaigns being run against other organisations as well. • Existence of 2-step verification for all accounts on social media from which our sites are managed. • Existence of good passwords on social media accounts and their safe keeping (in “Keepass”). • Adherence to other security procedures related to security on social media (we do not share passwords to unauthorized persons, we do not remain logged in outside working hours, we conscientiously share content on the pages we manage, etc.)
Resources and action of threat response:	• In case of direct threats addressed to activists/journalists – we inform the lawyer, the police, we publish the news / issue a statement regarding the threat, we contact NUNS; we enter the information in the internal and shared databases on threats. We take a screenshot of the threat. • In case of a negative campaign – we inform the lawyer (to ask for advice), publish the news / issue a statement regarding the threat, we contact NUNS, enter information in the internal database on negative campaigns. We are to conduct research of who is behind the negative campaign. • We remove negative and threatening comments from posts about our event after we take a screenshot. • If someone takes over an account on social media – we notify Facebook/Twitter, alert partners (by email), alert readers by posting on our sites and ask our partner organisations to do the same.
Emergency plan:	• In case of direct threats addressed to journalists – we contact the lawyer and the police. We inform the executive board and management board of our organisation. We take measures for the personal safety of journalists. • In case of a negative campaign – we contact the lawyer, inform the executive board, management board and issue a statement. • In case of intimidation of sympathisers by comments on social media – we remove the comments. • In case of taking over accounts on social media – we contact Facebook/Twitter, if they do not resolve the situation quickly – we contact the lawyer, the police and alert readers.
Quality of life plans:	• We provide support to a colleague who is the target of threats. If he/she needs it, we can pay for professional help (as an organisation). • We provide public support to a colleague who has been the target of threats – on social media and in public gatherings.
Required equipment and information:	• Internal database on social media threats. • Computer • Phone • Contact details of a lawyer • Contact list of partner media and organisations • Facebook and Twitter customer service contact

DIRECTION OF DEVELOPMENT OF SAFETY OF NGOs AND JOURNALISTS IN SERBIA

At the beginning, we said that the approach taken so far was wrong, and we noted the unsystematic approach as the major drawback, whereas the main advantage is good communication between journalistic organisations and NGOs regarding the issue. The development of safety for journalistic and non-governmental organisations, therefore, depends on overcoming the challenges of unsystematic approach and exploiting good communication practices.

Understanding safety as an essential function of non-governmental and journalistic organisations is a basic prerequisite for any safety system to be developed.

In order for such an opinion to become common, it is important to first observe all the consequences that organisations have suffered due to safety problems and dealing with them inattentively – starting from personal problems of activists and journalists, to the neglect of the basic functions of organisations which has resulted in solving some incidental security issues as unprepared as we are. In order for all the members of the organisation to take safety seriously, it is necessary, at least formally to begin with, to lay down the basics of a safety system – to designate a safety manager within the organisation, to make some initial security procedures, but also to begin with a detailed safety assessment and the development of serious safety documents. For a more serious understanding of safety, time should be allocated to discussing safety issues at every major meeting of the organisation and members of the organisation should be encouraged to attend safety related seminars.

Better reporting of safety issues of organisations is necessary to bring the public's attention to our position, to alert other organisations to a certain safety issue, and to resist media attacks that support safety threats. Therefore, regular safety procedures should include reporting on the organisation's website after each incident and contacting like-minded organisations and the media to also publish news or share our announcement. We should also be obliged to report to donors on all safety issues so that they have an understanding of the possible postponement of our project commitments and possibly provide us with a project to purchase security equipment.

Separation of the safety budget is necessary in order to respond appropriately to the threats. The budget does not have to be too big – before you draft it, always think of alternative, less expensive solutions (e.g. a "baby camera" instead of a CCTV system) that can reduce the

risks at least in the first period. It is important that you make a safety analysis and prioritize (which we talked about at the beginning of the guidelines) before budgeting. Increasingly, donors are opting for safety grants, but again you need to keep pointing out all the problems you face.

Safety education is essential at all levels. At the individual level, every member of the organisation must know at least everything about their role in the organisation's security system. The organisation itself must take the time and resources to organize internal training for all employees, while NGOs dealing with safety must devote themselves to adequately educating NGO activists and all journalists at risk.

Insisting on better understanding by state authorities is necessary in order to enhance cooperation in the field of safety, first of all with the police, judicial authorities and law enforcement bodies. We will achieve this by inviting state authorities to respond whenever the safety of NGOs and journalists is threatened, but also by insisting on increasing the number of activities of joint bodies of NGOs and journalists and state authorities concerned with safety issues.