

P reventing and r eacting to aggressions

Purpose:

Assessing the likelihood of different kinds of aggression taking place.

Preventing possible direct aggression against defenders.

Carrying out counter - surveillance.

Aggressions against human rights defenders

Violence is a process, as well as an act. A violent aggression against a defender does not take place in a vacuum. Careful analysis of aggressions often shows that they are the culmination of conflicts, disputes, threats, security incidents and mistakes which can be traced over time.

Aggressions against defenders are the product of at least three interacting factors:

- 1 • **The party who takes the violent action and means.** Aggressions on defenders are often the product of processes of thought and behaviour we can understand and learn from even if they are illegitimate. The party will need to invest means at least to gather information (security incidents) about the target HRD.
- 2 • **Background and triggers which lead the aggressor to see violence as an option.** Most people who aggress defenders see aggressing as an "useful" way of reaching a goal or "solving a problem". Impunity and/or willingness to pay the political cost as "worth it".
- 3 • **A setting** that facilitates violence, allows it to take place or does not stop it. A quick way to and away the HRD.

Who, then, is a danger to defenders?

Generally, anyone who thinks that aggressing a defender is a possible, desirable, acceptable, or potentially effective way to achieve a goal can be considered a

potential aggressor. The threat increases if s/he also has, or can develop, the capacity to aggress a defender.

The threat of an aggression can decrease with changes in the potential aggressor's capacity to stage an aggression, their attitude towards how acceptable an aggression is, or how likely s/he is to be caught and punished.

Some aggressions are preceded by threats. Others are not. However, the behaviour of individuals planning a targeted violent aggression often shows subtle signs, since they need to gather information about the right time to aggress, plan how to get to their target, and how to escape.

It is therefore vital to detect and analyse any signs indicating a possible aggression. This involves:

- Determining the likelihood of a threat being carried out (see Chapter 1.3);
- Identifying and analysing security incidents.

Security incidents which involve surveillance of defenders or their workplace are aimed at gathering information. This information isn't always intended for use in an aggression, but it is important to try and establish whether it is or not (see Chapter 1.4). Surveillance can be used for a number of purposes:

- To establish what activities are carried out, when and with/by whom.
- To use this information later to aggress individuals or organisations.
- To gather the information necessary to carry out an aggression.
- To gather information for legal action or other harassment (without direct violence).
- To intimidate you, your supporters or other people who work with you.

It is important to remember that surveillance is usually necessary in order to carry out an aggression, but doesn't in itself constitute an aggression. Also, not all surveillance is followed by an aggression. Targeted violence does sometimes occur in situations when an aggressor suddenly sees an opportunity to strike, but even then some level of preparation has usually been carried out first.

There is little information available to help you recognise an aggression being prepared. The absence of studies on this subject contrasts sharply with the large number of aggressions against defenders. However, the studies which do exist offer some interesting insights ¹.

¹ Claudia Samayoa and Jose Cruz (Guatemala) and Jaime Prieto (Colombia) have produced interesting studies on aggressions against human rights defenders. Mahony and Eguren (1997) also carried out an analysis of such aggressions.

- ♦ **Aggressing a defender isn't easy and requires resources.** Surveillance is needed to establish an individual's movements and the best location for aggressing. Getting to the target and making an effective, quick escape is also vital. (However, if the environment is highly favourable to the aggressor, aggressions are easier to carry out.)
- ♦ **People who aggress defenders usually show a degree of consistency.** The majority of aggressions are aimed at defenders who are heavily involved in issues affecting the aggressors. In other words, aggressions are not usually random or aimless, but respond to the interests of the aggressors.
- ♦ **Geographical factors matter.** For example, aggressions on defenders in rural areas may be less public and therefore provoke less reaction at law enforcement level and political level than aggressions in urban areas. Aggressions against NGO headquarters or high profile organisations in urban areas generate a greater reaction.
- ♦ **Choices and decisions are made before an aggression.** People who are considering an aggression against a defenders' organisation must decide whether to aggress the leaders or grassroots members, and choose between a single hit (against a key, possibly high-profile person and therefore at an increased political cost for the aggressor) or a series of aggressions (affecting the organisation's membership). The few studies done on aggressions against defenders suggest that both strategies are usually applied.

Establishing the feasibility of an aggression

To find out how likely an aggression is, you need to analyse the factors involved. To establish what those factors are, it is useful to differentiate between different kinds of aggressions, i.e. common crime, incidental aggressions (being in the wrong place at the wrong time) and direct aggressions (targeting), using the three tables on the following pages ².

² This classification of aggressions includes the same categories as for threats: Please have a look at the chapter on threats for clarification.

Table 1: Establishing the probability of direct aggressions (targeting)

(PA stands for potential aggressors)

PROBABILITY OF DIRECT AGGRESSIONS (TARGETING)			
FACTORS	LOW PROBABILITY	MEDIUM PROBABILITY	HIGH PROBABILITY
CAPACITY TO AGGRESS	PA have limited ability to act in the areas where you work	PA have operational capacity near the areas where you work	Zones where you work are under the firm control of PA
FINANCIAL MOTIVE	PA do not need your equipment or cash for their activities	Interest in your equipment, cash, or other forms of financial gain (i.e. kidnapping)	PA in clear need of equipment or cash
POLITICAL AND MILITARY MOTIVE	None - your work has nothing to do with their objectives	Partial interest - your work limits their political and military objectives	Your work clearly hampers their objectives, benefits their opponents, etc.
RECORD OF PREVIOUS AGGRESSIONS	None or rare	Occasional cases	Many previous cases
ATTITUDES OR INTENTIONS	Sympathetic or indifferent attitude	Indifferent Occasional threats Frequent warnings	Aggressive, with clear and present threats
SECURITY FORCES' CAPACITY TO DETER AGGRESSIONS	Existing	Low	None, or security forces collaborate with (or become) PA
YOUR LEVEL OF POLITICAL CLOUT AGAINST PA	Good	Medium to low	Limited (depending on circumstances) or none

Example

of the probability of direct aggressions (targeting):

The PA control the areas in which you work, but they do not have any financial motive for aggressing you. Your work only partially limits their political and military objectives, and there are no precedents of similar aggressions in the city. Their attitude is indifferent, and they do clearly not want to attract any national or international attention or pressure by aggressing you.

The probability of direct aggressions in this scenario is considered to be low to medium.

Table 2: Establishing the probability of crime aggression

(CO stands for criminal offenders)

PROBABILITY OF CRIME AGGRESSION			
FACTORS	LOW PROBABILITY	MEDIUM PROBABILITY	HIGH PROBABILITY
MOBILITY AND LOCATION OF CO	CO usually stay in their own areas, away from your zones	CO generally enter other areas at night (or operate close to your work areas)	CO operate anywhere, day or night
AGGRESSIVENESS OF CO	CO avoid confrontation (predominantly commit crime where you do not stay usually)	CO commit crime in the street (but not in staffed offices)	CO openly commit street robberies and enter premises to commit crime
ACCES TO/USE OF WEAPONS	Unarmed or use non-lethal arms	Crude weapons, including machetes	Firearms, sometimes powerful
SIZE AND ORGANISATION	Operate individually or in pairs	2-4 people operate together	Operate in groups
POLICE RESPONSE AND DETERRENCE	Rapid response, capable of deterrence	Slow response, little success capturing criminals in the act	Police do not usually respond with even a minimum degree of effectiveness
TRAINING AND PROFESSIONALISM OF SECURITY FORCES	Well trained and professional (it maybe that they lack resources)	Regular training, low pay, limited resources	Police are either non-existent or corrupt (cooperate with offenders)
GENERAL SECURITY SITUATION	There is lawlessness but the situation is relatively secure	Lack of security	Rights not observed, absolute impunity

Example

of an assessment of probability of crime aggression:

*In this city, criminals operate in different areas in pairs or small groups, sometimes during the day. They are often aggressive and often carry guns. The police does respond, but slowly and ineffectively, and the police force is unprofessional and under-resourced. However, the police leadership is well disciplined. There is a clear lack of security, and if applied to the marginal neighbourhoods of the city, the probability of crime aggression is at its highest given that **all** the indicators are at high level.*

The probability of a criminal aggression in the centre of a city like this is at a high to medium level

Table 3: Establishing the probability for incidental aggressions

(PA stands for potential aggressors)

PROBABILITY OF INCIDENTAL AGGRESSIONS			
FACTORS	LOW CHANCE	MEDIUM PROBABILITY	HIGH PROBABILITY
YOUR KNOWLEDGE OF CONFLICT AREAS	Good	Approximate	You know very little about where combat zones are located
DISTANCE TO CONFLICT AREAS	Your work is far away from these areas	Your work is close to these areas and you occasionally enter them	Your work is carried out in combat zones
MOVEMENT OF CONFLICT AREAS	Conflicts zones are static, or change slowly and verifiably	They change relatively often	They change continually, making them unpredictable
YOUR KNOWLEDGE OF LOCATION OF AREAS WITH LANDMINES	You have good knowledge or there are no mined areas	Approximate knowledge	Unknown
DISTANCE BETWEEN YOUR WORK PLACE AND AREAS WITH LANDMINES	Your work takes place far away from these areas, or there are none	Your work is close to these areas	Your work takes place among mined areas
COMBAT TACTICS AND ARMS	Discriminate	Discriminate, with occasional use of artillery, ambushes and snipers	Indiscriminate: bombardment, heavy artillery, terrorist or bomb attacks

Example

of an assessment of probability of incidental aggressions:

In this area, you are familiar with the combat zones, which change slowly and verifiably. Your work is close to the areas where the fighting takes place and you occasionally visit or stay in the combat zones. You are not close to mined areas. The combat tactics used are discriminate and therefore do not affect civilians very often.

Work in this zone carries a low level of risk of incidental aggression.

Preventing a possible direct/indirect aggressions

Although the defender is the target in both cases, let's distinguish between:

- direct aggression against the defender
- indirect aggression against the defender when it involves someone close to the defender

In both cases prevention will require the same underlying logic.

You now know that a threat can decrease with changes in the potential aggressor's capacity to stage an aggression, their attitude towards how acceptable an aggression is, or how likely s/he is to be caught and punished.

To prevent an aggression it is therefore necessary to:

- ♦ Persuade a potential aggressor or a person making threats that an aggression will involve unacceptable costs and consequences;
- ♦ Make aggression less feasible.

This type of aggression prevention is parallel to the analysis covered in Chapter 1.2, which states that risk is dependent on the defenders' vulnerabilities and capacities. In order to protect yourselves and reduce risk, you need to take action against the threat, reduce your vulnerabilities and enhance your capacities.

When a threat is made and you want to reduce the risk associated with it, it is important to act - not just against the threat itself, but also on the **vulnerabilities** and **capacities** most closely related to the threat. At times of great pressure, when you want to react as quickly as possible, you often act on the vulnerabilities which are easiest to deal with or closest to hand instead of those which are most relevant to the threat.

Be careful: If the risk of aggression is high (that is, if the threat is strong and real, and there are several vulnerabilities and fewer capacities), working on vulnerabilities or capacities to reduce the risk makes little sense, because these require time to change and become functional. If the risk is very high (a direct and severe aggression is imminent) you can only do three things to avoid it:

- a** ♦ Immediately and effectively confront the threat, knowing that you can achieve an immediate and specific result which will prevent the aggression. (Usually it is very difficult to be sure that there will be an immediate and effective result, because reactions take time, and time is precious in this situation.)
- b** ♦ Reduce your exposure to as close to zero as possible, by going into hiding or leaving the area ³.

³ However, there will be occasions where attempting to travel might put someone at greater risk.

c ♦ Seek effective protection!: see two examples of what might be effective protection (depending on context):

- Community protection: if you hide or seek refuge in a community, public eye and witnesses might deter the potential aggressor.
- Armed protection: it might be somehow useful in a few cases, but assuming that it is close at hand (immediate), that it can deter the potential aggressor and that it does not put the defender in more danger in the medium or long term. Realistically, such requirements of armed protection are very difficult to fulfil! Some Governments offer armed escorts to defenders, after national or international pressure; in these cases, accepting or rejecting the escort may have to do with holding the state accountable for the security of defenders, but a Government can never say that it is relieved of its responsibilities if the defender does not accept the armed escorts. Private security companies may lead to more risk if they are linked to aggressors⁴ And for defenders, to carry weapons, we must say, is usually ineffective against an organized aggression, and may also make defenders vulnerable if a Government uses this as a pretext for attacking them on the basis of fighting terrorism or insurgency. Moreover, carrying weapons could be twisted against the defender as being in contradiction with the UN declaration on HRD.

Threatening situations that can lead to an aggression are easier to handle if other relevant actors or stakeholders become involved and work together. Examples include a functioning judicial system, support networks (domestic and international) that can put political pressure on duty-bearer stakeholders, social networks (within or among organisations), personal and family networks, UN/international peacekeepers, etc.

Surveillance and counter-surveillance

Counter-surveillance can help you establish whether you are being watched. It is difficult to find out whether your communications are being intercepted, and for this reason you should always assume that they are⁵. However, it is possible to determine if your movements and offices are being watched.

Who could be watching you?

People who are usually in your area, such as doormen or porters in buildings, travelling sales people who work close to the building entrance, people in nearby vehicles, visitors, etc, could potentially all be watching your movements. People do surveillance for money; because they are being pressurised to do it; because of their sympathies, or due to a combination of these factors. Those behind the surveillance may also place collaborators or members of their organisation in your area.

⁴ For more information please see in this Manual the chapter on "Improving security at work and home".

⁵ For more information see in this Manual the chapter on securing communications.

People can also watch you from a distance. In this case they are almost always members of an organisation and will probably use the tactic of watching without wishing to be seen. This means keeping a certain distance, various people taking turns and watching from different locations, using different vehicles, etc.

How to know if you are being watched

You can find out if you're being observed by watching those who could be watching you and by adopting the following rules (without, of course, becoming paranoid):

- If you have reason to think that somebody might want to watch you, you should be mindful of the movements of people in your area and changes in their attitude, for example, if they start asking about your activities. Remember that both women and men can carry out surveillance, as can old or very young people.
- If you suspect that you are being followed, it is possible to put in place a counter-surveillance measure involving a third party whom you trust, and who is unknown to those who might be watching you. This third party can watch, in advance and from a good distance, movements which occur when you arrive, leave or go somewhere. Whoever is watching will probably do so from a place where you can always be easily located, including your home, offices and the places where you most often do your work.

For example

Before arriving home you can ask a family member or trusted neighbour to take up a position close by (e.g., changing a car wheel), to check if somebody is awaiting your arrival. The same can be done when leaving your office on foot. If you are using a private vehicle, it will be necessary to have another car leave after yours in order to allow a potential observer time to begin their approach towards you.

The benefit of counter-surveillance is that, at least initially, the person observing you does not realise you know they are there. It should therefore be made clear to anyone involved in the counter-surveillance that it may not be advisable to confront the person observing you. They will then realise that you know about their activities, and this could also provoke a violent reaction. It is important to take the utmost care and keep a distance if you are aware of somebody watching you. Once surveillance has been detected, you can take the action recommended in this manual⁶.

Most of this counter-surveillance advice applies almost exclusively to urban and semi-urban areas. In rural areas the situation is very different, but defenders and communities who live in such areas are more used to being aware of strangers nearby. It is therefore more difficult for somebody who wants to watch you to gain access to inhabitants of a rural area - unless the local population is deeply hostile towards your work.

⁶ See chapter on "Improving security at work and home"

Note: building a relationship with the security forces monitoring you could be beneficial in some circumstances. In some circumstances the surveillance will not be a secret as part of the point is to make it visible/intimidating. In some situations defenders cultivate people in the security forces who can sometimes tip them off when surveillance or even an action is planned against them

When to check if you are being watched.

Logic dictates that it is wise to check if you are under surveillance if you have reason to believe that you are - for example, because of security incidents which could be related to surveillance. If your human rights work carries a certain risk, it is a good idea to conduct a simple counter-surveillance exercise from time to time, just in case.

You need also to think about risk you bring to others if you are under surveillance – the risk may be greater for a witness/family member of a victim you are meeting than for you. Think about where would be most secure for them to meet. You may need to warn them that your movements might be under surveillance.

Reacting to aggressions

No single rule can be applied to all aggressions against defenders. Aggressions are also security incidents, and you can find guidelines for how to react to security incidents in Chapter 1.4.

In any kind of aggression there are two essential things to remember:

- Think always about security! Both during and **after** the aggression. (If you are under aggression and you have to make a choice between two alternatives, go for the safest one!)
- Following an aggression, it will be necessary to recover physically and psychologically, take action to solve the situation, and restore a safe work environment for you and your organisation. It is crucial to retain as much detailed information as possible about the aggression: what happened, who/how many people were involved, number plates of vehicles, descriptions, etc. This can be useful to document the case, and should be compiled as quickly as possible. Keep copies of any documents handed over to the authorities to document the case.

Summary

Aggression is the culmination of a process which definitely included security incidents, maybe threats.

Thus aggression is not an “unexpected” event.

Aggression can be incidental or targeted

It is not easy to aggress human rights defenders as they are public figures and enjoy some kind of support.

Aggression is the product of 3 interacting factors:

- The party who takes the violent action and means
- Background and triggers which lead the aggressor to see violence as an option
- A suitable setting

An aggression requires adequate resources and capacities, access to the individual, a quick escape and a certain level of impunity or the decision by the aggressor that it is worth the political cost.

Therefore, preventing an attack requires actions both to maintain the political cost as high as possible (reduce impunity level) and to reduce one’s physical exposure to risk as close as possible to zero.

