Infiltrators, Informers and Grasses

how, why and what to do if your group is targeted

.: w w w . a c t i v i s t s e c u r i t y . o r g :.

For more information, extra copies or requests to do talks (UK only) please email us at info@activistsecurity.org

If you think your group has a leak, and you want help or advice, please feel free to contact us, but remember that unless you are using GPG/PGP your emails are not secure – our gpg key is available on request. For advice on security in general please visit our website and download the free **Security Handbook for Activists**.

1st Edition, Summer 2009

Introduction

It is never pleasant to think that one of the people you are working with, possibly very closely, who you go drinking with, who is sleeping with one of your friends, who seems so full of life and passion is actually trying to undermine everything you are doing.

Unfortunately, if your group is challenging often very powerful industries or people with vested interests it is inevitable you will make enemies along the way. And in a number of cases they will retaliate or seek to counter your campaign, regardless of how small or large it is. Anyone who has been campaigning for some time will have those moments when someone or something just does not chime right, when suspicions are raised that all is not going well. This booklet is a guide for turning suspicion into certainty.

We first discuss the likely sources of threat, what they are after and the different techniques they use. This is followed by collecting the evidence to turn suspicions into fact. Thirdly, we explain how to challenge a suspect and present findings to your group. In the last few sections we look at specific situations, such as new people, collaborators and gatherings, which have particular issues.

Some cautionary words

It really is an unpleasant task having to deal with informants, and often reactions get very emotional. Some people go into denial, refusing to believe it; others get very angry and want to take pre-emptive action. These are both natural reactions, but neither are helpful.

If you get the presentation wrong you can end up breaking a group or cause a witch-hunt of an innocent individual. Unfounded paranoia is not helpful to anyone but your enemies. Indeed, paranoia is not part of the security process; it is an unhelpful state of mind often built on emotion. Your fears need to be grounded in facts and rational consideration to be part of your security in a useful way. You need to be able to back them up with more than vague hypotheticals that can justify any position you are taking.

Fortunately, the problem of insiders working against us is not as big as we might suppose, and those who sponsor them spread disinformation about the extent of it. It suits their purpose to keep people guessing. It is always good to remember there has been and remains a long history of successful campaigns and actions despite the informers operating inside our groups.

It does not matter if your group is very open rather than closed and covert. There is still much that a skilled operative can do to cause disruption to make you

ineffective. For example, planting false information such as at the Heathrow Camp for Climate Action's plenary, or journalists deliberately twisting your unguarded words. Just because you have nothing to hide does not mean that you are going to be able to avoid the issue, it just means you have different methods to deal with dishonest intentions.

If there is one thing to take away from this booklet it is to always have proof before you start making accusations against someone. Witch-hunts based on insufficient evidence and vague rumours have ended up destroying groups.

Calling someone a snitch is a very serious charge to lay at anyone's door. The personal consequences can be a backlash against yourself, or even causing your group to split. It is never to be done lightly; do not mention it jokingly in conversation behind someone's back as that is how nasty rumours begin. Even passing on accusations made by others without real factual backup or research is to be avoided.

Individuals who constantly make up this sort of accusation about those who disagree with them, or even on personal grounds, need to be challenged as this acts as to poison the group as a whole. This has been a deliberate tactic developed by state agents (acting both overtly and covertly) to disrupt enemies or dissident groups.

A classic example, dated now, was to forge a letter from one member of a group making allegations against another to cause internal dissent, and then spread rumours that the letter is a fake. Impossible to get to the bottom of, the result is a group that implodes trying to find out the actual truth, dividing along personal and political allegiances. Fortunately, this has become fairly obsolete, but it is an illustration of the levels that the State is willing to go to. Read Machiavelli.

Disinformation from the police is also a factor to concern yourselves with. They are aware that a group closing in on itself, drawing away in paranoia and mistrust is effectively dead. So they will let it "slip" that some of their success has come from an inside source in order to create the divisions that allows them to break your group and individuals down.

Often it is guesswork or intelligence gathered from other sources such as listening devices and tapped telephones, carefully shaped to make it look like they know more than they do. Take care and tread carefully before making allegations, do not do their work for them.

If in doubt, find independent people who have had experience dealing with informers and infiltrators and get advice from them before leaping to conclusions.

Everything we talk about in this booklet we have had personal experience of, or we have spoken directly to people who have gone through it. The danger of informers and infiltrators is a very real threat; numerous campaigns have been disrupted because of them, and many more people have gone to jail because of this sort of betrayal and targeting.

It is not about how peaceful or innocent your group is, these tactics have been used on everyone from peace groups to militants irrespectively. What matters is who you are upsetting. Do not expect your opponents to share your knowledge or logic – often they do not understand those they are targeting and may have the wrong picture altogether of the sort of a threat you actually pose. It is fair to say that they rarely understand the concept of non-hierarchy, and often they are actually working from a position of ignorance.

Breaking it down: infiltrators, informers and grasses

In this booklet we use the following definitions for convenience.

> *Infiltrators* – individuals who insert themselves for the purposes of gathering intelligence; as often amateur as they are professional, but generally they have no prior connection to the group or true concern for the issues. Generally motivated by ideological opposition or money.
>
> *Informers* – members of the group who have been "turned" or induced to betray the group, whether to avoid criminal charges or for money. Some are simply people with addictions (alcohol, drugs, gambling debts) who are manipulated into talking.
>
> *Grasses* – people who have been turned after an event, often following an arrest, but it can be for other reasons. They are used to provide evidence against (former) colleagues, or to entrap them.

Infiltrators are expensive for the police to run and more likely to be favoured by corporations with deeper pockets. Informers and grasses, are preferred by the State as they are cheaper than employing someone full time and without the attendant risks.

Who is paying and what they want

The types of agencies that will seek to infiltrate a group come in three distinct groups: the State, corporations and the media.

The State

State agencies will be the most professional and experienced of the threats facing you. They target those they think might be involved in criminal activity in furtherance of a political agenda, are actively organising political protests or even just might upset the status quo. Their goal is not simply solving crime or policing protest, but as much about gathering information, building profiles and on occasion simply disrupting the group to the point where you are no longer a threat.

It is not helpful to see the State as a single entity with a clear agenda. Different parts do things in different ways with different objectives and budgets. Various arms of the State are funded to different levels and often they are in competition with each other. So just because some parts are well funded, it is a mistake to think that all are. Different police forces have their own agendas and how they spend their budgets on surveillance, infiltration or even just targeting groups will vary greatly.

Secret services and national groups (eg. MI5, FBI) often have long term objectives, based on evidence gathering and disruption; they tend to be resource rich. The information they want is a working knowledge of who the key people are, their details and habits, and how the organisation as a whole is structured.

They are significantly more prepared to bend the law, and their agents will try to get in deep to the heart of the organisation, putting in a considerable amount of work to get into place. Their agenda is often to do with large social movements which threaten the status quo, regardless of how avowedly peaceful their tactics.

Local police are in general resource poor and focus on immediate results, such as arresting as a crime is taking place, or removing from circulation a particular group of activists. They are restricted by rules on entrapment and the need to get quick results to justify budgets.

As a rule of thumb the secret service branch of government generally runs infiltrators while local police prefer to use cheaper informers and grasses.

All branches of the state can be utilized for political purposes, such as the targeting of groups successfully embarrassing the government, acting to protect their political masters over and above the solving of any crime. Collaborating to pass on information to powerful corporations has been well documented, despite that in many cases this amounts to a breach of the law.

Corporations, Lawyers and professional agencies

A very different beast from the State again, their objectives are quite varied and often money is no object. Usually their objectives are one or more of:

a) finding information on forthcoming campaigns so that they can successfully pre-empt threats including through PR, or sabotage the group's activities;

b) information gathering on people and campaigns for threat analysis;

c) preparation for legal cases.

Most corporations outsource this to professional companies who come in various sizes. Some, such as Knoll, are trans-national and do as much work in industrial espionage as on campaigns against particular corporations. Other smaller companies such as Global Open, Verity, etc. are staffed by ex-policemen putting their skills and personal knowledge of campaigners to use.

In some cases these professional companies are acting at the specific request of companies who fear protests. However, a significant number are proactive and

seek to gain information on campaigns which they can turn into (often very inaccurate) reports to sell onto companies.

Connected to this group are the lawyers seeking dirt on groups or specific information on which individuals to target with legal actions. Some, such as Lawson-Cruttenden & Co are known to have reciprocal relationships with private investigation firms. The paperwork in court cases such as these can be very useful sources of information and provide hints as to whether they have been using infiltrators or not.

On the whole, experience indicates that private investigators are much more likely to use infiltrators than informers. Occasionally they will work with the police, but their agents are often much more unscrupulous as they are not bound by the same codes as the police, and the latter see them as competition.

The Media

It is far from unknown for newspapers to get involved in groups to get a juicy story or to back up something they have heard and to do it covertly. Often easy to spot by their inappropriate clothes and their poor questioning technique – they struggle not to ask directly what they want to find out – and even by their open note taking. Some simply want photos. Pretty much all want a speedy story so they rarely invest the time and money needed to get away with it properly.

A nuisance more than anything, they are unlikely to give you a good press anyway. The best thing to do is politely ask them to leave.

Do you have an infiltrator?

Why would you suspect you have an infiltrator in the first place? Consider

- Things go wrong when they've not been doing so previously.
- Your opponents seem to know what you are planning despite your precautions.
- Constant internal disruption.
- New faces at meetings acting dubiously.
- Your opponents have a history of targeting campaign groups (in some situations/groups it is good to be pro-active before any damage is done).

It is rare that straight away there is clear proof you have an insider working against you. Sometimes the information comes from other groups who have noticed problems with yours, or have had a similar experience, or are even aware of a particular individual being a problem. In many cases it is simply pure instinct – you know something is wrong and you cannot put a finger on it, at which point you start digging to confirm or deny.

However, the first question to ask is: could the events that have aroused your suspicions be based on intelligence gathered through other means such as phone taps, bugs and so on. The more of these you can eliminate from the start the better. Looking for infiltrators should be at the bottom of the list.

Infiltrators tend to go for positions where they can either get the most information or do the most damage. Watch out for the following behaviour:

Information gathering

a) Volunteering for tasks which give access to important meetings and papers such as financial records, membership lists, minutes and confidential files, including typing up notes and 'recycling' the paperwork. Often they quite dull tasks so people are happy to pass them on to others despite how much they expose details of the group's members.

b) Asking probing questions bordering on the intrusive, particularly about people's personal details and actions questioner was not involved in. This allows them to build up a picture of people's roles in the group.

c) Regularly being overgenerous with money, including financing stuff or buying people drinks and/or drugs to gain access to activists socially with the aim of gaining their confidence or just causing them to become talkative.

d) Being insistent on giving people lifts home, especially when it means they are going out of their own way.

e) Regularly praising key people to their faces.

f) Regularly coming to meetings, joining discussions in the pub, but never getting involved in the group as such.

Disruption & discrediting

g) Not following through on, or completing, important tasks; or doing them poorly despite an obvious ability to do good work.

h) Causing problems for a group such as committing it to activities or expenses without following proper channels; or encouraging the group to plan activities that divide group unity.

i) Seeming to be in the middle of personal or political differences that are disruptive to the group.

j) Seeking the public spotlight, and then making comments or presenting an image different from the rest of the group.

k) Urge the use of violence or breaking the law, and provide information and resources to enable such ventures, but never quite get involved in the actions they have facilitated setting up. This depends closely on the nature & atmosphere of your group. Context is important here, especially how heavily monitored the group is.

l) Charge other people with being agents, (a process called *snitch-jacketing*), thereby diverting attention from him or herself, and draining the group's energy from other work.

m) Recommending or bringing around people of dubious character.

n) Where they have control over important information, they are obstructive in letting others sharing it in to the point important tasks are not able to be done.

o) Offering to supply key equipment which they do not follow through with, or else is of consistently poor quality.

Inconsistency

p) Having no obvious source of income over a period of time, or having more money available than their job should pay; eg. an expensive car.

q) Inconsistent about their background – lies at this level are hard to maintain completely, and slip-ups do occur; take note of inconsistencies and follow up any 'facts' they tell you.

r) Making false claims and exaggerating their roles in other movements.

s) Going out of their way to avoid answering questions about their home, family life, jobs.

t) Often disappearing for several days at a time – regularly happens with local police infiltrating as they have other work to do.

u) Have partners who suddenly disappear out of their lives as if they barely existed, to be replaced by someone in the group.

v) Live in houses that do not have feeling of being "lived in" – sparse details about themselves, lacking in photos, etc.

w) Seeming immunity from prosecution.

x) If the infiltrator is from the media they will often deliberately put forward mad ideas in order to create a more exciting response or story, in order to set up opportunities for their stories.

Remember, none of the above is by itself proof someone is an infiltrator. It may be that information is leaking through carelessness or surveillance on you. That someone is disruptive by nature, power hungry, or a pathological liar does not mean they are an informer, but they do need to be dealt with appropriately. There are also those people who are genuine control freaks and will disrupt if they cannot get their way within a group, and end up destroying it out of petulance rather than deliberate mischief. We do not cover it here, but it is a security issue in some ways as it causes others to become disaffected, feel betrayed, etc. The main thing is not to let it continue unchallenged to the point it affects your group's work.

Another source of information for State and companies are those who are security risk in themselves. That is, they do not have a personal sense of other people's security or refuse to acknowledge it as an issue. Alternatively, they may not be able to help themselves from boasting to increase their stature or get very

talkative when drinking with strangers for what ever reason. They may not actually realise they are a liability.

Likewise, people aware of an action but not directly involved in it, rarely share the same sense of security in relation to it as those involved as they are not directly at risk. They can inadvertently jeopardise actions or activists as a result. These people are not informers in the common sense, but the effect is the same. How the group deals with this will vary, but sometimes it will require a degree of harshness as there are more important things at stake. If it becomes known other groups will stop working with yours, or the group may split over the matter. This is a possibility where some members want to end their association with the individual, while others wish to continue working with them, whether because of personal history or political reasons. The best approach is transparency – discuss it out together rather than in small cliques.

Initial Action & Gathering Evidence

Once you are sure your suspicions have substance, check with a couple of others whom you trust to check you are not alone. If several of you feel the same way, all independently then that is a good sign there is something afoot. With them on board, the next stage is to gather evidence to back up your suspicions.

1. Contact someone experienced for advice (legal and practical), or a professional group such as Buro Jansen & Jansen (www.burojansen.nl).

2. Put processes in place to protect sensitive material or planned actions; often if you close off the information supply your suspects have been accessing they may soon drop out anyway, solving one problem.

3. Create a file of question marks over the suspect(s), noting all the evidence you are gathering. This should include accounts of suspicious events and statements from people. It is worth doing this even if you have not identified particular suspects as it helps identify patterns. Record dates, time, places, people present and other material that puts the event into context. Note disruption of actions, eg. the unexpected presence of police. ***Keep this safely stored, preferably encrypted or using codes – think of the danger of it falling into the wrong hands!***

4. Discreetly inquire about their background and personal life and check it out. This is probably the most important part of the investigation, and subtlety is paramount here to avoid tipping them off. Never discuss it openly on phones, email, etc, in case they are being monitored as well.

   It is very hard for infiltrators to lie consistently all the time, especially if you are probing in areas where they do not have a cover prepared. Remember, cover stories tend to be a mix of both truth and lies. Make notes of any inconsistencies, but allow for the fact that people often exaggerate anyway just to fit in. If several people are doing this (though not all at once!) then a better picture develops.

5. If they claim to be, or to have been involved in other groups, speak to them, maybe taking a photo in case the suspect has changed their name. Often when an infiltrator has been exposed in one group, they simply move onto other ones in related movements, using their experience and contacts to make the transition easier. However, watch out for other groups tipping off your suspect, so be careful if you are approaching third parties for help and ask them to stay silent.

6. Check out their claims by contacting their 'employer', or following them home. Something is probably amiss is when a person drives an old car to meetings, but can be found driving something much newer at home, or the place of employment cannot be found. If they are being secretive make excuses to visit their home, or arrange surveillance of them. More sophisticated operations will have these basics covered though.

   In some situations it is useful to distract the person and go through their possessions, including phones and computers, to see if there is anything incriminating – particularly useful at gatherings or meetings where there is limited time to evaluate someone. If you have access to where they live then check out their bins, diaries and personal spaces such as bedrooms, which often have giveaway clues (eg. a "vegan" with meat wrappers in the bin).

7. It is always useful to visit their relatives were possible. Infiltrators often try to keep family away from the group they are targeting, and in some cases it has been family who have let slip useful clues.

8. As you progress in confirming your suspicions approach others you implicitly trust to help build your body of evidence. We really emphasis caution here, as it is hard to prevent people's suspicions from leaking into meetings and social events. However, if several people already suspect a person independently then that is a good sign you are on the right track – as long as it is not just on the grounds that the suspect is simply new and particularly keen or does not have great social skills. Beware also that jealousy might sometimes be a factor.

9. Be aware of people simply jumping on the bandwagon and agreeing with you uncritically. Constructive challenges to your assumptions are worth having; but at this stage it should be on a need to know basis.

10. Set a trap. "Arrange" an action or meeting that the suspect is informed of and check to see if there are any police or extra security waiting. If the subject is talking about their involvement with others in the group this may be tricky to organise. It needs to be planned carefully, and may need to be done more than once to catch the person out, especially if they are in for the long term as they will wish to avoid raising suspicion before they have had a chance to properly integrate with the group. Also one set of unexplained extra presence can be explained away as bad luck; more than once ceases to be coincidence, though it may be bad security practice on the behalf of the suspect such as talking openly over the phone about it – in which case you have a liability anyway.

    Avoid acting too out of character so as not to tip them off that it is a trap, or doing it in a way which may arouse suspicions from others in your group that

there may be something worth investigating.

Often in such a set up the suspect, if they are working for the State, etc., will back out rather than do something incriminating. Either way you know they are not up for it and not to be given trust lightly.

11. If you suspect you have an agent provocateur, consider getting them to incriminate themselves – have a dictaphone ready so when the opportunity arises you have evidence, in case anything is used against you in the future, that it was the infiltrator or the grass who tried to entrap you. Keep the recordings secure (not in your house) and make backup copies. Maybe talk to a lawyer you can trust. Most police infiltrators will try to avoid being active in anything that may be construed as illegal as this will compromise their evidence in court – especially if it can be argued they instigated it or had a chance to prevent it. Private investigators will be less inhibited.

This is an extreme action and we really cannot recommend that you carry a dictaphone around as it puts other, genuine, activists at risk. Never do it for genuine actions you are involved in. Plus if people notice you might be the one who ends up getting suspected. *Only do this if you have a very strong belief that someone is attempting to set you up.*

When investigating someone it is easy to convince yourself that they are guilty because that is the basic premise you are working on. Be open to being challenged that you might have got it wrong or that what you have assembled simply is not sufficient. So the last part of this stage is to bring in an outsider who can evaluate the evidence from an experienced and independent viewpoint without the same emotional attachment you have, and who has credibility with others.
You want your case to be as water-tight as possible, but saying that, it is often very hard to get that sort of evidence. Sometimes you can only ever be, say, 80% certain that you have the right person, in which case it is even more important to get an external review before going public.
Never go public on insufficient evidence – what happens if you get it wrong! You could lose a person who could subsequently be turned against you, and you can end up creating a bad atmosphere in your group, disrupting your effectiveness. You also will lose credibility and may even have people turn on you.
If you got it wrong, even before you go public, be prepared to admit it, especially if you have spoken to others. Make a point of going back to them and stress that the suspicions should remain confidential. Otherwise these things have a habit of getting out through careless talk, which does nobody any good.

Exposing the infiltrator

Meeting with the suspect

When you have gathered what you feel is sufficient evidence, the next question is the appropriate manner to act upon it. How this is done depends on the horizontal/vertical nature of your group. For hierarchical groups, speak to key people you feel can be trusted with the information and ask them how to proceed.

For non-hierarchical, grassroots groups, which we are focusing on, the best approach is to get the information out to the group as a whole, which you need to plan for.

The first part is to arrange a meeting between a few of you with the suspect and put your evidence before them. Ideally bring in an outsider who had no knowledge of the suspect to act as facilitator and/or to make independent judgement.

Watch the suspect's reactions and carefully note their explanations of the evidence. Be ready to listen and present calmly; it is not the time to go in all guns blazing and making accusations before the evidence is present. You need to keep in mind that they might actually be innocent, and that this process is going to be very insulting and upsetting for them. Avoid your own hubris.

However, normally, by this stage the evidence should be sufficient that their game is essentially up – though they may not actually accept that, which can result in arguments and them shouting that it's all a hoax, that they cannot work under these conditions, and so on. If you are going to publicly expose them afterwards get a photograph of your infiltrator while you still can.
Either way you need to be ready for their anger and for them to throw accusations back at you.

Going to your group

Next, arrange a full meeting of your group, and put the case before them. It is wise not to announce the true purpose of the meeting beforehand as others talking to your suspect may inadvertently tip them off. When talking about the meeting in advance do so only in the most oblique terms (eg. a "significant security issue has come up").

Ideally the meeting challenging the suspect will take place shortly before the meeting with the group as a whole. If they do come to the meeting to defend themselves, they will be better prepared and change their story to adapt to the evidence, so you will have to challenge them on this – this is the main reason for

having witnesses at the initial confrontation, and they should come to the group meeting as well.

As with the initial meeting with the suspect it is important where possible to have outside facilitators and a clear sense of process.

At the end of the meeting, ask the suspect to leave the room so the rest of the group can come to a consensus on which side they believe. It may be worth you leaving as well to avoid claims of bias. If they agree with you, then ask the infiltrator to leave the group.

If there is no group meeting
There are two situations here. One is where the infiltrator has left still asserting their innocence. The other is that given geography, security etc, there are good reasons why it is not possible to call the group together physically. In both cases there are very good reasons for you to take immediate action.

The infiltrator may attempt to get in first and poison the group against you, turning the tables so that it is you who ends up justifying your behaviour, not them. They may also make it a personal thing that affects the group dynamics. The other issue is that the sooner you begin dealing with the fall out the healthier it is all round.

The two key things at this point are:

(1) Primarily, providing straight away to your group the information to back your claims up. It is important that things are clear and transparent to ensure that you are not seen as abusing power.

(2) Also, you will undoubtedly have to explain to some group members why they have not been trusted with this information to date, as they may be hurt by the perceived lack of confidence in them.

Inconclusive evidence
If you cannot find strong proof for your suspicions, you need to approach the matter differently. A potential approach is to confront the person with your suspicions as it may be enough for them to back off, but be prepared for the situation to backfire and they deny everything (after all they may be innocent).

Perhaps do it partially, to get them to confirm or deny a part of their story, doing it gradually rather than confrontationally so you can back off without raising too much suspicion if there is a material change or they have provided satisfactory explanations. Continue to monitor them if necessary.

Dealing with the fallout

Once the infiltrator has been exposed you need to protect your reputation and to repair the damage to your group:

(1) Consider going to the press to highlight the issue. The appropriateness of this depends on the nature of your group and is often better suited for more mainstream groups with a policy of staying within the law.

(2) Let other groups know through established channels. Publish a photograph of the person on relevant websites and other news services (magazines, Indymedia, etc.) so others are also able to identify the infiltrators. Exposing "burning") an infiltrator like this can put them out of the job for good. Always substantiate your accusations. Send a letter to the groups you are connected with giving an explanation and what you are planning to do to minimize the problem. An example of how one infiltrator was exposed and advertised is the first "Notes from the Borderland" by Larry O'Hara, which deals with the activities of the infiltrator Tim Hepple/Matthews.

(3) Expect some uninformed backlash and loss of reputation, but it is better this happens than people finding out through rumour which will affect your credibility even more. The real danger you face here is rumours spreading unchecked and nobody being able to verify claims and counterclaims.

(4) Put in processes to prevent it happening again. This will help protect your reputation following any backlash over the exposure of the infiltrator. It is more important to be seen to acknowledge mistakes and being pro-active about rectifying them than trying to keep it secret. You can come away stronger as a group if it causes you to adopt better and more sustainable security practices.

(5) Change locks, passwords, protocols, etc. and analyse the effect on materials and campaigns they may have been involved with.

(6) There may be further questions relating to other individuals that the infiltrator has brought into the group, and time may need to be put aside to deal with this.

(7) Act to minimise the damage to your group. This is important to stop unnecessary paranoia and infighting that can arise – especially where some members do not fully believe the gathered evidence or where there have been relationships between the infiltrator and group members.

Some group members may not want to accept that they have been conned in this fashion and their objections may be based on this. Others may be deeply traumatised so you need as a group to come together for them.

As important as anything else is to look after yourselves. It is horrible when it happens, so look after each other and deal with the emotional side of things so that you can come out stronger. Do not try and bury it away and pretend it did not happen. At least have a meeting to talk about it openly.

New people

Many people when they first get involved are often excited by what they have read and heard. They may not have had a chance to adjust to our security culture and needs. It does not make them spies, and jumping down their throats immediately – or not explaining the situation to them because you've gone into paranoid mode – does nobody any good. You are more likely to lose enthusiastic people.

What may seem obvious to us is only so because of our experience as activists; it may not be that way to an outsider so allow them that initial space. Explain to them first! We were all young, naïve and eager to take action once, so think back to what it was like then, and the mistakes that you made.

The main thing is to avoid letting paranoia take over. People do not join a group fully clued-up, so don't expect them to be. A group with so much paranoia that it is it actually impossible to join is not going to go far. This sort of paranoia also prevents accurate instincts from developing.

Saying that if they truly believed new people would put up with the paranoia and exclusion is a poor excuse and symptomatic of a group which is not dealing with security on a rational level.

If your group is genuinely concerned about new people coming into it, for whatever reason, then develop a process bringing them in, testing them and skilling them up. You can be cautious and welcoming at the same time. Wait until you get to know them before actually making pre-emptive judgements.

If they still do not get it, then is the time to become somewhat more concerned. If your campaign is structured securely, a grass or infiltrator should only be able to achieve limited damage, plus you should not be exposing new people to sensitive material anyway. It is always good to visit people at their homes or just learn about their backgrounds. Maybe even meet their parents if such an opportunity arises. This helps builds up trust.

Gatherings

These pose a different set of problems. However, final authority normally rests with the organisers, or a sub-committee specifically set up to deal with this issue, to ask the suspects to leave. You do not have much time to gather evidence, but in our experience spotting them is not particularly difficult as they have a tendency to stand out due to not having done enough research on how to fit in.

Ideally a couple of people will get together and agree on a strategy for dealing with the person, including approaching them with questions (either confrontationally or subtly as the occasion requires). Some of these people should be recognisable individuals or organisers to give the group doing this some standing in the eyes of the rest of the gathering, or else it should be convened and authorized by a spokes-council where appropriate.

The last thing you want is a debate on the process when you are actually trying to have an infiltrator leave, or a self-appointed mob trying to deal with the situation.

Ask the following questions about the suspect person:

- When they take notes at what point do they do it?
- Are they taking notes in shorthand?
- Who are they watching and listening to? How keen are they on particular individuals and at writing down people's names?
- How are they making approaches to people? What sort of questions are they asking of people; are they showing repeated interest in illegal or violent activity, or being exceptionally nosy about people?
- Are they asking questions about 'leaders' or that simply do not sound right (eg. "Where is your central communications unit?")
- What about their clothes, watches and shoes (eg. leather at an animal rights event)?
- How did they arrive, and who with? Have they walked and left an expensive car out of sight?
- Who do they appear to know, if anyone at all?
- How clued in are they to the cause? Are they making elementary mistakes?
- Do they appear to be drinking but actually are nursing the same beer throughout the night?
- Have they professional journalist equipment with them such as dictaphones and cameras?
- How have they learned of the event, and what are their reasons for attending?
- Who do they claim to be in contact with?
- If you decide to go through their bags and tents, have they ID which identifies them as someone else, or recording equipment?

Generally infiltrators at such events come singly or in pairs and do not know anyone else there. They can latch onto a group of people and act as if they are part of the same group, something that is easy to check out. Simply because they are hanging out with others does not necessarily mean that they are their friends. We have even dealt with situations where they have come from other countries.

What often happens in these situations is various people start to get suspicious of an individual and start pointing them out to the various organisers, etc. This is why it is worth having at least one or two people working on this who can take the various feedback and then make the decision to investigate further or not. Likewise, if someone is being unnecessarily paranoid then their fears can easily be laid to rest by locating the suspect's friends, if they exist and checking them out.

The simplest thing to do is to just strike up a conversation with the suspect and gently question them. It leads to a much better idea of how genuine they might be. It is quite easy to do this in a gathering-type situation, but remember to avoid taking an aggressive stance at this point as it is counter-productive. You want them to be relaxed and feel able to communicate with you. Give them the feeling that they are making contact so they will open up a bit more in return.

In a number of cases, a suspected individual has been able to provide *bona fide* credentials on questioning and demonstrated that they were a genuine member of a group in attendance once they were challenged, so do not march individuals straight out of the venue. Always give them a chance to be vouched for.

If an infiltrator has been identified to people's satisfaction, escort them out of the venue immediately. Experience has shown that escorting them round to get their stuff causes more trouble than it is worth. Tell them that it will be brought to them once they are outside the venue. Use reasonable force to eject them but do not get excessive. Initiating a scrap in this situation is counter-productive on all levels, as people have different expectations or may see it as something other than dealing with an infiltrator and step in to intervene.

Most will leave of their own accord having been spotted, but some will kick up a fuss (journalists are quite bad for this) thinking to raise support from others at the gathering in the hope that it will cause you to back off. This is why having processes prepared in advance for this sort of eventuality is very useful, especially were there might be divergences in opinion on inclusivity, media strategy, openness, etc.

If there are people at the gate/entrance make sure they see the person to avoid letting them back in later on. Taking photos of the individual is good for later identification, so if they do manage to get back on they can be easily re-identified.

Grasses

Sadly every now and again activists will give in to police pressure / persuasion and agree to work for them against your group. It is not always used directly against you, but there are signs you can watch out for.

Commonly when people turn grass ('singing') in a post-arrest situation they are separated from the other defendants. 'Public Immunity Certificates' [PICs] may then be issued to prevent the fact that they are talking being made public. They do not even need to be a defendant, but can be a different member of the group.

Often their evidence will not be used directly, so it may not be immediately apparent that this has happened. Your solicitor should be informed if a PIC has been issued, but is supposed to not to tell you, though it usually becomes clear as it opens up a gaping hole in the evidence. PICs may also be granted in favour of witnesses you wish to call to support your case which means they cannot be summoned. As a rule of thumb you should be very hesitant to trust anyone who has a public immunity certificate issued for them.

Other evidence that someone has turned is the quality of treatment they get when arrested. For example, one turncoat received a TV in her police cell when she agreed to make a statement against other people also arrested.

Likewise, where the grass is up on charges by themselves, they may get ridiculously low sentences. Other signs are that the police suddenly know where to target people effectively or can quote very specific evidence in interviews.

It should be made very clear that anyone who gives a statement against other activists will be made very unwelcome by the rest of the movement. They should be named and shamed along with having their photos published in relevant forums. However, if they are part of a larger trial, this should not be done until after the end of the trial to protect other defendants (it is their call as they are the ones who will suffer the worst).

A standard tactic used by police during interviews is saying that your mates have given statements implicating you. This is generally untrue and it is better if you stick to any position agreed in advance, such as "no comment" interviews.

Other 'infiltration' methods

The Media

If someone approaches your group outside of actions or press releases, as media seeking to do a story on your group or campaign, immediately check their credentials. Film & TV production companies are a good front to approach

activists in an attempt to get close to them.
Ask for their cards, and phone the switchboard of the newspaper/TV/radio station they claim to work for to check they are genuine. Mobile numbers are not good enough to trust; what you want are office lines. In more sophisticated set-ups the phone number will also be genuine in so much as it will go to a switchboard, so check their presence on-line or in the phone-book to confirm their identity and that the numbers are indeed going to genuine offices.

Do some basic research into their background and be very suspicious of media companies which do not have much presence online or in trade journals, and do not appear to be involved in any other productions. Ask for references, and check that they too are *bona fide*. Where possible arrange to visit them in their offices. Be wary of insistent requests to visit offices and to meet other activists (especially those involved in direct action), and deny them whenever possible.

Sometimes the approach may be genuine, but the media is always looking for the exclusive footage and 'inside scoop', so they have a completely different agenda to the campaign or group. They have been known to set people up, so you should always be on your guard around them, and be very careful about how much information you provide. Carefully manage what they are allowed access to and when they can record. You do not have to give them everything they ask for and you are under no obligation to cooperate. Once you stop feeling comfortable with them end the contact.

Given the prevalence of video-cameras these days there is little reason for mainstream media to be on covert actions at all, regardless of their demands for exclusives. If the story is good enough, your footage will be picked up anyway.

Decoys

If the State has gone to some effort and expense to put someone well placed within a group they will use tactics to protect that cover. The simplest is to back off on arrests to allow them to build up a level of trust within the group.

Another is to use a more obvious person to act as a decoy for the group to focus on. So while everyone is laughing at the very obvious cops in the pub they are forgetting about the less obvious one sitting among them. It is not always used, but it is one to watch for.

Likewise if the police are letting it slip that they have infiltrators or informers the question to ask is, why are they giving away the fact that they have a valuable asset in the group? The chances are that it is to deliberately confuse or build mistrust.

Other campaign groups

Other agencies can be front organisations set up to get your trust, so just because you are dealing with someone from another organisation with supposedly the same aims as yourself, unless they have a proven track record then treat them carefully when passing on details about yourself, etc. Even if they are a proven group, they may have an unspotted infiltrator or slack security, so pass on personal or sensitive material with care.

On being approached by the police

This happens all the time and it is not something to be scared of. The police will make offers of reduced prison sentences or money, or may simply threaten. We know of cases where it has been crude blackmailing threats, including against other more vulnerable people, if there not cooperation with them. It is vital you do not give in to them. Nod, learn what you can from them, take the number they will give you, then walk away without making any commitments whatsoever. It is okay to take their cards with their numbers, but circulate it later.

Once they have left you alone, have a nice shower and tell friends as soon as possible. Consider posting on Indymedia, or if you are feeling confident, make contact again and tape what they have to say and publish that.

We never recommend playing the game of feeding them false information. It is not worth the stress or money and the police are likely to take it personally.

Protect yourselves

One very successful infiltration operation involved someone going to various campaign groups and offering to recycle their waste paper, and passing on their discoveries to companies, including personal details and campaign strategies. Concern about infiltration is pointless if you are leaking information from poor security processes.

In many cases where infiltrators have been suspected, the actual problem turned out to be that the group was making it too easy for others to put them under surveillance or gather information. If you give them an easier option the chances are that they will take it. For more information on anti-surveillance or setting up the appropriate security processes see the Activist's Security Handbook.

Final notes

There are two important points to finish on.

It is just as often the problem that people on seeing something suspicious do not act. They assume it is someone else's responsibility, or that it is simply too horrible to contemplate that someone might be there for all the wrong reasons. Yet letting someone go unchallenged is to nobody's benefit in the long run. There is no point in saying, after someone has spent years causing damage to a group that you suspected them all along because of some incident. You are just as much at fault for not dealing with it at the time.

The other point is that gossip is destructive. We cannot emphasise enough how dangerous it is to idly speculate with a group of friends about whether someone might be a grass or informer without substantiating it. It is detrimental to a group's internal dynamic and invariably the subject of the gossip will hear about it or pick up on it. The allegation should never be made lightly or without proof.

If your friends or fellow group members are doing this then you need to call them up on their behaviour. If they cannot produce anything of substance, then explicitly tell them that it is insufficient and the conversation should stop. If you have suspicions, then investigate them. Sitting around a pub table with a small clique of you spreading unsubstantiated rumours is simply a whispering campaign, intentional or not, and is no better than organising a witch hunt.

Alleging infiltration, informing or grassing is serious and not to be placed lightly at anybody's door. Nor is it acceptable to ignore the evidence that your group might have one. As we said at the start, it is an unpleasant business, but a very real problem many activists have had to deal with over the years.

Hopefully this guide will have given you a good handle on approaching the issue.

For more information

The Activist's Security Handbook, www.activistsecurity.org
Eveline Lubbers, "Battling Big Business".
McLibel, http://www.mcspotlight.org/issues/freedom/index.html
IMC: www.indymedia.org.uk, www.indymedia.org.nz, portland.indymedia.org
Public Eye: in particular www.publiceye.org/liberty/whatbugs.html This article is also useful for US readers on where they stand legally with respect to infiltrators and spying.

Thank you to everyone who has spoken to and trusted us over the years, and who let us learn from their mistakes.