Investigating Intelligence Activities

Investigating Intelligence Activities

Intelligence agencies can appear hopelessly impregnable. The information is inside the walls and we are on the outside. But security is usually more impression than reality. In every government agency (and private companies), no matter how strict the security, the secrets walk in and out of the doors every day as people go to and from work.

Don't assume that all intelligence officers are the same. Every organisation has a range of people, with a range of political and ethical views, some of who may welcome the opportunity to talk.

Finding insiders willing to help you get information is a matter of persistence and, partly, luck. Word of mouth is the most successful way of finding people, but lots of work can be done to increase the likelihood of hearing of potential sources.

Intelligence officers have the usual network of family, friends, neighbours, professional contacts, old university colleagues, sports associates and so on. These are the people from whom we hear about people in intelligence jobs and whether they seem open-minded. Leads can be actively sought from people in relevant university departments (eg. languages, mathematics and computing for intelligence agencies), elsewhere in the same general profession (eg. information technology specialists), in the public service union and in the military. Obviously, towns and cities near intelligence facilitites are good places to look. Note too that sometimes an intelligence officer speaks out and is reported saying a few things in the news, but no one ever thoroughly interviews them to gather all their other stories and insights. Approach them.

For me, staff lists have been the key to getting inside intelligence agencies. Some of this information was compiled from scattered sources, but the most came from finding intelligence officers' names hidden within military staff lists. This provided the structure for all my research.

Investigating staff can feel obtrusive, but we can ensure that no personal information is ever used. For instance, knowing staff can give clues to the locations and sizes of intelligence operations and to overseas postings to allied intelligence services. In one case, studying the location of staff allowed me to discover a large but previously unknown interception site. All kinds of unclassified or low-classified lists might be useful: government pay records, government job advertisements, union membership lists and so on.

Internal phone directories can be extremely useful: for instance military phone directories, which are not very secret, include many people who assist intelligence activities or may come from or go to an intelligence job. Public telephone books, lists of registered voters, registers of property owners and published university results can all help trace people.

Even very secret information is usually located in more than one place and some of those locations are easier to assess than others. For intelligence, interesting information may be found in other government agencies, around senior politicians, in the military (which is generally much less secretive than intelligence agencies), in companies providing technical support and equipment and even in allied countries. It pays to draw a matrix of the information you would like and all the possible places it could be located.

I never telephone a potential source the first time, as it is too hard to establish trust and not scare them off. Even getting an introduction through a mutual friend may feel too insecure. After researching the person, I usually visit their home – turning up on their doorstep – and introduce myself and explain what I am trying to achieve. The key is establishing trust (and being worthy of it). These approaches have usually worked.

Secrecy is a necessary part of intelligence research. Intelligence staff are given stern security "indoctrinations" and are not allowed to talk about work even to their families. They risk serious trouble if caught talking to you. So, right from the start, contact must be made carefully. The person must be sure that their identity will be protected for the rest of your life. Most ordinary people are hopeless at keeping secrets (which is a mostly good thing), so it's essential to keep secrets to the absolutely minimum number of people.

Knowing names of many intelligence staff helped me in an unexpected way. Insiders who might have been too scared to be the first person to spill the beans, found it easier to talk when I knew the names and could talk about their work mates. They felt much more comfortable when they were talking to someone who knew their world and were just "adding" to my knowledge rather than being the first or primary source.

Interview techniques – insiders will usually have stories on their minds they are keen to tell, but getting most information takes careful interviewing. Because you probably don't know what there is to find out when you start, the key is asking a wide range of detailed questions (eg. on equipment, targets, organisation structures, personalities, regulations, manuals, links with foreign agencies, intelligence successes, things that went wrong, the layout of facilities…). The key is asking the right questions – and detailed questions can be a trigger for your source to remember other things. It is on the second or third interview, after reading over your interview notes, that you might strike upon the crucial questions and get the most valuable information.

Reading other publications on the subject can help suggest lines of questioning. Note that all western intelligence agencies adopt very similar procedures and techniques, and lots of training, manuals and operations are shared between them. So revelations about one agency are a guide to what is likely in the one you are studying.

Since most insiders cannot be quoted by name, and documentary evidence is rare, it is difficult to give credibility to inside information. How do we prove to sceptics that it is correct (especially on a subject where lots of silly stories fly around)? My solution was to gather such a wealth of detailed information about the workings of intelligence agencies that the revelations had internal credibility.

I build trust with sources by telling them in advance that they retain control over all information that they give me. This means that I take drafts to them to check that they are comfortable with what I used and that they cannot be recognised as the source. I remove information if they ask and are the only source. This checking pays off for me too as they often spot errors and add more information. This is how I first heard of Echelon!

When publishing, put yourself in the mind of the agency security officer, who studies the dates your various pieces of information cover and which sections it could have come from and tries to narrow down suspects who may have talked. Mix up information from varied sources and omit details that point to just a few people.

Don’t underestimate field work, and don’t over-estimate security. Carefully studying intelligence facilities, the network of facilities in different countries and changes over time can produce valuable information. For instance, you can often see the direction that listening antennae are pointing and watch changes to intelligence facilities over time that match developments in telecommunications networks.

Don’t assume that security cannot be bypassed. Very secret information calls for unconventional research methods. Also don’t be fearful: there is far more personal risk from exposing, for instance, a rough, small-time criminal than from probing intelligence services.

The obscurity of the issue means that there are numerous scattered sources that have never been put together. Workers in technology companies, university departments and the military all have gossip and maybe know people you could talk to. Our job is to ask around and gather the pieces. Clues, like a memorable tiny detail I once noticed in our Army News, can lead to whole new areas of discovery.

Technical advice, for instance from contacts in the IT and communications world, can explain the communications systems which the spies are targeting and help you piece the story together.