I.M.R. Handbook - Trade Craft [1]

Now, there are five sorts of spies. These are native spies, internal spies, double spies, doomed spies, and surviving spies. When all these five types of spies are at work and their operations are clandestine, it is called the "divine manipulation of threads" and is the treasure of a sovereign.

Native spies are those from the enemy's country people whom we employ. Internal spies are enemy officials whom we employ. Double spies are enemy spies whom we employ.

Doomed spies are those of our own spies who are deliberately given false information and told to report it to the enemy. Surviving spies are those who return from the enemy camp to report information. Of all those in the army close to the commander, none is more intimate than the spies; of all rewards, none more liberal than those given to spies; of all matters, none is more confidential than those relating to spy operations. He who is not sage and wise, humane and just, cannot use spies.

And he who is not delicate and subtle cannot get the truth out of them. Delicate, indeed! Truly delicate!

There is no place where espionage is not possible. If plans relating to spy operations are prematurely divulged, the agent and all those to whom he spoke of them should be put to death. Generally, in the case of armies you wish to strike, cities you wish to attack, and people you wish to assassinate, it is necessary to find out the names of the garrison commander, the aides-de-camp, the ushers, gatekeepers, and bodyguards.

You must instruct your spies to ascertain these matters in minute detail. It is essential to seek out enemy spies who have come to conduct espionage against you and to bribe them to serve you. Give them instructions and care for them. Thus, double spies are recruited and used. It is by means of the double spies that native and internal spies can be recruited and employed. And it is by this means that the doomed spies, armed with false information, can be sent to convey it to the enemy. It is by this means also that surviving spies can come back and give information as scheduled.

The sovereign must have full knowledge of the activities of the five sorts of spies. And the key is the skill to use the double spies...
-- Sun Tzu, "The Art of War"

This guide is intended to have two uses. To give some suggestions as to useful tactics to employ in the pursuit of our goals, and also to warn you of tactics your opposition may take.

The Bodyguard

The two basic principles of security are that the target is primarily responsible for his own safety, and that the security measures should be commensurate with the threat.
A number of principals delegate their safety to professional bodyguards. However, unless tied to their principal by blood, or members of an elite unit with exceptional *esprit de corps* (such as the US Presidential Protection Unit), bodyguards can be bribed or blackmailed into betraying their patron -- all it takes is a moment's hesitation when the moment comes. Naturally, the bribes are hardly ever paid; the corrupt bodyguard is traditionally killed himself as part of the attack. The bodyguard's employer will often test his loyalty by getting a third party to approach him with a false bribe.

Mad Bombers

The trained agent refers to home-made bombs or incendiaries as Improvised Explosive Devices or IEDs. These are normally hidden carefully and appear as a common-place article like a piece of luggage. Anyone with any exposure at all to IEDs knows that moving, opening or tampering with them can set them off; unless you have a reasonable Demolitions skill your action should be to put it down gently on the nearest flat surface (if you've somehow picked it up), clear the area (opening the windows if possible), and get help from the authorities. A surprising percentage of people don't realise this and can be counted on to kick the device, shake it, carry it to the nearest police station, or immerse it in water.

Usually, bombs are used to frighten or injure people (such as IRA car-bombs), whereas incendiaries are used to destroy property (such as the Animal Liberation Front's firebomb attacks on department stores selling furs). The threat of either can be used to disrupt travel and business without the expense or inconvenience of actually planting one.

The majority of devices used by terrorists and criminals are simple, and built from common household items such as watches, flash bulbs, and clothes pegs; more organised groups make use of stolen military supplies to assemble bombs requiring a high degree of technical knowledge. The home-made items have a fairly short shelf-life; complex devices with military explosives and electronic timers can be planted months or years in advance of use.

[1] Adapted with thanks from : http://www.geocities.com/pentapod2300/best/spies.htm

You Can Drive my Car

The professional expecting trouble -- or a principal advised by one -- is very nervous around his vehicle. He checks the garage for nasty surprises before entering, and the car itself before getting in; knowing what to look for and how to search takes about a day to learn and the check itself takes under two minutes. He prefers to have a choice of several vehicles and routes for any trip, and will avoid establishing a pattern in his use of either. He is alert for strangers or unknown vehicles, and records their descriptions to pass on to police or friends.

He avoids narrow streets or ravines, stopping, or slowing down, especially if anything unusual like an accident occurs ahead; he will turn off and choose another route instead, and is prepared to accelerate away at the first sign of trouble, usually with lights and horn going to attract attention. Minor breakdowns like flat tyres are ignored until a known safe place is reached. If attacked by another vehicle, he will avoid driving alongside it (which risks a broadside) or trying to force it off the road, into a ditch etc. (which locks the vehicles together and makes him a perfect target).

Secure The Area

Building or site security has four main components: A detection system of some sort to warn you that intruders are coming, communications to relay information and orders, delaying barriers to slow down the intruders until they can be dealt with, and response forces to deal with them. These are countered by three main strategies: stealth (sneaking in without setting off the alarm), deceit (convincing the guards or systems that you should be let in), and the brute force approach (overwhelming the site with sheer numbers and firepower).

Sensor Readings

Detection includes not only alarms and sensors, but the way that you control access to a site -- checkpoints, gatehouses, and so on. Access restrictions (e.g. checking passes) are aimed at entry by deceit; barriers are used to deal with entry by stealth or force. Alarms and sensors are deployed just outside the barriers, so that you run into trouble as soon as you've tripped the alarm.

Walking Through Walls

The barriers are there solely to delay the intruder; they are not expected to stop him on their own. Given time, the defenders will test their barriers thoroughly, and can be expected to know to within seconds how long it will take a determined adversary to break through; if they can afford it, they will have sufficient response systems or forces to get there no later than the time you break though the last barrier and with enough force to stop you cold. Barriers are normally arranged in layers; for example, a fence surrounds the building, and the McGuffin is in a safe inside a locked room in the sub-basement. Barrier design also aims at forcing the intruder to use complex, expensive equipment and highly-skilled people to break through; if you have to get a nerdy computer technician, a thermal lance and a portable generator over the fence while wearing gas masks it's going to take longer and cost more. Making intruders squirm through a series of small holes is a especially good for slowing them down.

Fences range from four strands of barbed wire marking a boundary (just stroll on by) to wire mesh topped with razor wire and backed by mounds of concertina razor wire ten metres wide and three metres high (bring gloves, a ladder and bolt-cutters; scramble over in under a minute, or cut your way through in about 10 minutes). Electrifying the fence doesn't slow the intruder down, but does make mistakes more dangerous. Adding minefields slows him down (many minutes if he sneaks in, less than two if he blows the mines up and pulverises innocent bystanders within 250 metres of the fence).

Walls (Cont'd.)

Walls range from clay tiles (smash a hole through with a sledgehammer in under 60 seconds) through 20 cm reinforced concrete (2-7 minutes with power tools, a couple of minutes with explosives) to 50 cm expanded metal and concrete bank vault liners (spend all night at it with hand tools, or bring your own antitank weapon).

Intruders with vehicles are harder to stop. The barrier ranges from the common motorway barrier to concrete tank-traps; getting through one of these means ramming them with a one-ton truck doing 80 km/hour, and being prepared to write off the truck afterwards. Ditches and revetments are also used; it takes around 30 seconds to stop the vehicle, erect prepared ramps or bridges, and drive over. As ramming is less effective at lower speeds, crash barriers or parked vehicles are often placed in front of walls or gates to protect them.

The sort of building you'd want to break into has a roof made of some combination of metal subdecking, reinforced concrete, insulation, wood sheathing and waterproof membranes. Depending on thickness and materials, penetration time using hand tools ranges from 3 minutes to longer than you'd wait; explosives take 2-3 minutes, but you might get caught in the blast. Power tools big enough to be useful are too heavy to get onto the roof. Once you're inside, floors are basically thicker roofs without the waterproof membrane.

Most doors can be penetrated in less than a minute using hand tools (axes, crowbars) or small explosive charges, and mechanical locks can be picked or burned out in under 30 seconds. Vehicle access doors are best defeated by ramming. For the serious paranoid, the "King Tut Block" comes highly recommended; when you leave, you use a truck-mounted crane to emplace a multi-ton concrete block over steel beams in the floor, right in front of the door; then you drive off in the truck, presumably laughing. Bank vault doors take 10-30 minutes to defeat by stealth, depending on what you use and how good they are; explosives will get you through in under 5 minutes.

Regardless of whether it is standard, tempered, wire reinforced or laminated, someone with hand tools and a bad attitude can be through a glass or acrylic window in under 20 seconds. Polycarbonate windows last nearly two minutes. Adding steel bars or mesh inside the window adds a minute or so to penetration time. Without doubt, the window is the weakest part of the building, and the prime target for attacks. The usual response is to make them too small to crawl through.

Heating/ventilation ducts, sewers and so on are another weak point. Intruders can move through them at roughly half to one metre per second if horizontal, and about half that if vertical. Ducts in secure buildings are filled with barbed wire or wire mesh screens (decreasing speed by a factor of 15 as you have to cut and remove the wire), or metal grids (quartering speed).

Guards! Seize Them!

The response forces vary greatly in quality depending on the employer. Major government or corporate sites have teams trained and equipped to deal with suicide squads of terrorist fanatics; they will neither show nor expect quarter. Protection at less important sites ranges from nothing at all to a couple of guard robots with an Artificial Intelligence watching all access points by video camera. The guards' response time varies on whether the owner wants intruders intercepted before they reach sensitive areas, before they get their hands on the McGuffin, or before they can get back out again. It is also strongly affected by their motivation and alertness.

Under Lock and Key

Mechanical key locks have been around since the 18th century, and most can be defeated in under 30 seconds with simple tools; even the most secure offer no more than a few minutes delay to the skilled intruder, and if he is careful you will never know he picked the lock. However, key locks are easy to make, easy to repair, and adequate for keeping animals or small children at bay, so they remain in use even in the 21st century.

Combination locks are more secure as there is no direct access to the mechanism. Since the 1950s (when manufacturers stopped resting the fence on the edge of the tumblers) it has not been possible to pick them using a stethoscope. Since the late 20th century, the tumblers have been made of plastic or ceramics to resist decoding using portable X-ray machines. The impatient can melt the lock with thermite, make it brittle with cryogenic fluids then shatter it, or blow it up; any of these takes under two minutes, and melting done skillfully (you just melt the mechanism without damaging the casing) is not obvious to a cursory inspection.

Electronic coded locks require an ID card, PIN number, or scan of the user's retina or hand geometry to allow entry. They typically control electromagnetic latches in the door frame capable of withstanding 1,500 kg of force. Someone with skill and a security systems kit can be through in 10-30 minutes; brute force also comes highly recommended.

Interrogation

There are two main approaches to interrogation: Trickery and torture. Each has its supporters; some say that enough pain will loosen anyone's tongue, others that careful and repeated questioning exposes the truth better, arguing that someone being tortured will simply tell you whatever he thinks will make you stop, which is not necessarily the truth. The approach chosen by your captors depends on their skill, their personal preferences, their organisation's regulations, and how much time they think they have.

Most people with experience in this line of work know about the classic "good cop - bad cop" routine, and are taught to make themselves "the grey man" -- to convince their interrogators that they are unimportant cogs in the machine, weak, stupid, frightened, and ignorant of whatever the interrogator wants to know. They are also trained to have several layers of cover story in place, so that if the outer cover story is broken, they have a plausible second one to fall back on, and so on. Unfortunately, the interrogators get the same training.

The result is usually a test of endurance and willpower. The captive sticks to his original cover story as long as possible, to buy his colleagues enough time to realise he has been captured and take appropriate action; then pretends to have broken under interrogation, and reveals his second story, hoping to persuade the inquisitor that this is the truth, at which point the interrogation will stop. The interrogator meanwhile uses lack of food, lack of sleep, and possibly torture to rattle the prisoner so that he makes mistakes, thus revealing whether his current story is the truth or not.

Most people will break eventually, though not all. Since it has proved impossible to discover who will hold out and who won't, no one is told more than he needs to know for his mission; what he doesn't know, he can't be made to tell. Occasionally "doomed spies" are given false information and deliberately betrayed to the enemy by their own superiors, so that when they are interrogated the enemy will find out the disinformation and act on it.