During this phase, the handler will instruct the agent how to make contact and how to avoid being followed. The agent will be shown how to construct and mark a dead-letter drop and how to use a variety of equipment in order to help solicit the information, such as miniature cameras. If the agent is being used for sex, they will then be instructed in the use of covert recording equipment. The handler rarely provides the agent with guns or explosives; it may well provide the agent with a means of getting rid of him should things go wrong. In all cases the handler will do his best to stick with his cover story and will continue to be as friendly as possible with the agent while continuing with the monetary rewards. If the handler thinks that the agent is getting too close to him and that the operational security is at risk, then he may well pass the agent on to another handler. It is vital that the agent never gets the chance to break off contact and they can never be allowed to quit or resign.

▲ A sexually compromising situation can be a good lever when trying to recruit a new agent.

Sex can be a useful tool during the recruitment stage. It can be used to coerce someone to turn traitor or it can help manipulate someone into a compromising position. In many cases, sex can be a more effective tool than money, alcohol or drugs. Heterosexual compromise is used by many of the world's intelligence agencies. This starts with a simple introduction, i.e. putting a glamorous-looking woman in the same room as the target. One thing leads to another, with the end result being compromising photographs. The same applies with homosexuals; the beautiful woman is simply replaced by a pretty boy. Not all "honey traps", as they are commonly known, rely on photographs; the woman may say she is pregnant or the young boy may declare that he has AIDS. Both will be untrue, but they will serve to put extra pressure on the target.

A non-sexual compromise could come in a variety of disguises, such a criminal actions or security violations. The handler will exploit any of the agent's known compromises. If the promising agent has a clean past, the handler may well stage an event in which the agent is alleged to be a guilty party. Witnesses will be found, normally other agents under the handler's control, to provide evidence that proves the proposed agent to be guilty.

Whatever method the handler uses to co-opt the services of the agent, once achieved he must also provide some basic tradecraft training. It is in the handler's interests to make the agent as security-minded as possible and to ensure that the required objectives are being carried out correctly. In order to keep the agent firmly on his side, the handler must make sure that he can deliver any monetary or favourable promises. The agent's sole purpose is to do the bidding of the handler. Where this requires technical assistance, the handler must supply the agent with the necessary equipment and teach him how to use it. This may be a covert camera for bugging the agent's workplace or firearms, if an assassination is required. The recruitment of an agent is a long and dangerous game. Bearing this in mind, a good agent will need to be protected, even if this means that the handler has to prove assistance in any emergency.

DOUBLE AGENTS

When a spy enters a foreign country it is always possible that they have been recognized and put under surveillance. Instead of picking the spy up, the foreign agency may wish to keep them under surveillance and even try to implant a double agent. This double agent, commonly referred to as a "mole", will put themselves in a position where they can be recruited by the spy. A classic mole is one who has been recruited by the spy and then discovered by the opposition. When discovery is a choice between death or being a double agent, then the latter is often preferred.

For this reason the spy must ensure that anyone he recruits is genuine and test them accordingly. This testing phase is normally done by a specialist counterintelligence officer. This person will know how to detect and neutralize attempted penetrations by enemies of your organization. This normally means feeding some sensitive information to the new recruit

– and only to the recruit. It is simply a matter of waiting to see if this information comes to light from another source. For this reason it is best not to overuse new recruits until they have proved themselves.

CASE HISTORY

A car was stopped at a routine police checkpoint in Northern Ireland; the driver was a known villain on the fringes of a terrorist cell. There was no evidence to arrest the man and the police simply reported the matter to Special Branch. The name of the female passenger was also provided. She turned out to be the wife of a convicted terrorist currently in prison.

An operation was set up and compromising pictures were taken of the couple in bed at the woman's home. The next time the car was stopped, both of its occupants were shown the photographs and both were given the clear message that the woman's husband would shortly be getting copies. The consequences would have been severe for both of them; the woman may well have been disfigured, the man kneecapped.

The man was taken from the car by the handler dressed as a policeman and a deal was struck where the villain would supply information. The required information was deliberately kept simple and would not compromise the villain, who thought he was getting off lightly.

The following week the villain met with the handler at a motorway lay-by. The handler asked the villain to get into his car in order to discuss the requested information. This would only have taken a few seconds and the handler would have assured the villain that the pictures would be destroyed. At the same time, he pulled out a wad of notes and handed it over to the surprised villain. Thinking the Northern Ireland police force to be stupid, the villain went on his way £1,000 richer as a result of giving a useless piece of information.

Two days later the villain was stopped again. Somewhat agitated, once again he agreed to get into the handler's car. This time the handler showed him the pictures of him receiving the money, taken by a hidden camera. The penalty for sleeping with an interned terrorist's wife was kneecapping, the consequences for being a police informer would have been a bullet in the head. As it turned out, the SAS did a legitimate hit job on one of the terrorist cell members and the recruited villain was promoted in the cell. The rest was easy.

AGENT CONTACT

Once a spy has recruited his agent, he will need to meet him in order to issue instructions and to collect intelligence. This procedure is called "agent contact". Under normal circumstances, a handler working in a foreign country must assume that he is under surveillance. In order to set up a clandestine meeting with the agent, he will go through a set of procedures to ensure that an enemy surveillance team is not observing the meeting. Both the handler and the agent will have previously agreed upon a place, a date and a time or they will have set up a signal that indicates a meeting is to take place. In addition, they are familiar with each other's appearance, i.e. they can recognize each other on sight. The handler will provide the agent with a set of unique communication codes; this may be defined by hand signals, actions or clothing. The agreed signals will have various meanings such as, "We need to talk" or "I am under surveillance". A normal meeting between a handler and an agent would follow these basic steps.

STEP ONE

Both arrive independently at the previously agreed general location. Rather than fixing a specific location, they agree to be only in the general vicinity. This is an important principle. In this example, they are using a large park in a residential district. The location is free of video surveillance cameras. Ideally, the location should also be out of range of telephoto lenses. Other locations could include bus stops or a convenience store.

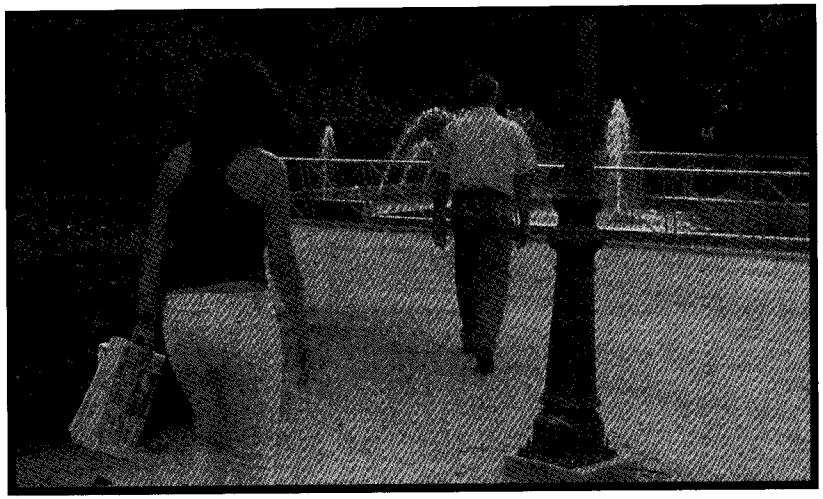
STEP TWO

▸ Agent contact – make eye contact.

Both the handler and the agent make discreet eye contact at some distance from each other. The handler, being the senior of the two, may use a prearranged signal to tell the agent that he has spotted him, such as moving a newspaper from one hand to the other or lighting a cigarette. The signal must be a movement that does not attract the unwanted attention of any enemy surveillance operators. It is important for both players at this stage carry out their surveillance with just one or two people; later they will literally surround their target with very large numbers.

STEP THREE

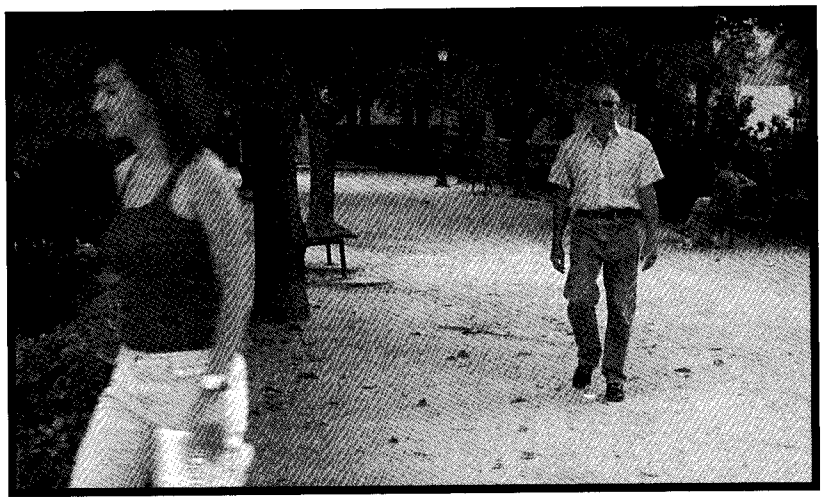
Once the recognition signal has been established, the handler will simply walk off, leaving the agent to follow at a distance. This ensures that the handler is clean and that he has not grown a tail. Surveillance teams on foot work on what is called a "floating-box principle". This means that they would form a very loose formation around the subject they are following. All main entry and exit points to a particular location will also be covered.



▲ Agent contact – check to see if I am followed.

STEP FOUR

When the agent has satisfied himself that the handler is clean, he will make a signal to him. This will usually be the carrying out of some everyday task, such as re-tying his shoelaces. Now the roles are reversed, this time the handler follows the agent to establish that he is also "clean".



▲ Agent contact – signal all clear, now check me.

STEP FIVE

▸ Agent contact – the meet.

When the handler is satisfied that neither he nor the agent are under surveillance, he will give the signal to meet. On the other hand, if either the handler or the agent suspects that a surveillance team is in the vicinity, they will simply abort the operation and walk away. Once they meet, they will discuss any issues and agree upon the date, the time and the location of their next clandestine meeting. This will also include several back-up plans in case that meeting is thwarted by surveillance.

ACT INSTINCTIVELY

It is vitally important to trust your instincts, because if something appears to be suspicious it is better to be safe than sorry. Many people are surprised to learn that it is not difficult to detect a surveillance team. If the agent requests a meeting with his handler, the latter must be careful that he is not being set up. Such a request by the agent is known as a "blind date".

PASSING MESSAGES

Messages can be passed in any number of ways. They can be done visually, in order to avoid contact association between the handler and the agent, or they can be covertly delivered. Over the years, both handlers and agents have devised numerous ways of passing messages. I have outlined a number of different techniques below:

HOLLOW COIN

▸ **Paying for goods or services is a "natural" way to pass a message on, especially when it is hidden in a hollow coin.**

Every country in the world has a currency system in place in order for the population to carry out their daily business, such as buying food, eating in cafes or paying for everyday goods. This is a natural transaction and one that is exploited by spies. Say that the handler needs to meet with his agent. He walks down the street and buys a newspaper, or stops for a coffee. The very action of buying a newspaper or a coffee requires that money change hands. If the newsagent or waiter is the contact, what better way to pass a message?

SOURCING MATERIAL

You can get your own hollow coin by purchasing one from a store which sells magic tricks.

A DEAD-LETTER BOX (DLB)

A dead-letter box is commonly referred to as a "DLB". It is a precise place where a message, or any other material, can be covertly left by one person and be collected by another. The aim of the DLB is to transfer a message without either parties making contact, thus avoiding being observed by others. The DLB can be located in almost any place providing that the placement and the pick-up can be carried out naturally. Placing a container in the ground, under a park bench or in a trash can have all been used. The secret of a good DLB is ingenuity.

DLB PROCEDURE

While each country has its own methods for teaching DLB procedures, the one devised and perfected by the KGB is the best example of how it should be done. Providing both the sender and receiver have proficient skills in counter-surveillance techniques, conforming to the KGB method will guarantee safe delivery.

THE DLB LOCATION

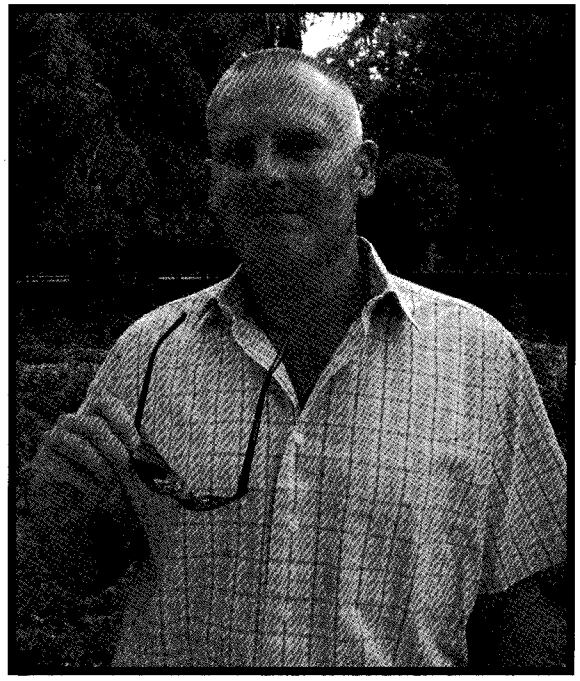
The spy will find a good location where he is are temporarily unseen by any surveillance team. He chooses his spot either to fill or to insert a DLB position or a container. He will always choose a location that is populated, such as a park or public transport, and avoid isolated places. He will then find places close to the DLB, but far enough away to avoid suspicion, where he can leave a signal that either the DLB is ready for filling, that there is material in the box that the material has been picked up. These signals should be foolproof and unspotted by any surveillance team.

Several DLB places should be known and agreed to by both the handler and the agent. Likewise, a timing system should be in place for each DLB drop. The time spent in the area should be limited and the pick-up should never take more than 15 minutes. To increase security for a DLB, the handler and agent should have a number of fake DLB locations. These

should be worked into the handler's or the agent's normal daily routine. All the handler and the agent have to do is to walk past these fake DLBs on a regular basis.

STEP ONE: READY-TO-FILL SIGNAL

Once the delivery device is made, the spy cn pass information to his handler. Assuming that a predetermined area has been agreed on, the first step is for the agent to signal that he is "ready to fill" the DLB. This might take the form of a chalk mark or a piece of chewing gum stuck on a park bench. The idea is to produce a signal that can be seen clearly but which is virtually imperceptible to the general public's eye.



Ready to fill signal.

STEP TWO: READY-TO-PICK-UP SIGNAL

Once the handler sees the ready-to-fill signal, he will make a ready-to-pick-up signal. As with the agents "ready-to-fill" signal, this will normally involve something simple, such as lighting a cigarette or making a chalk mark. On seeing this, the agent will place or fill the DLB. Once this task has been done, the agent will then remove his ready-to-fill signal. By doing so, he is simply informing the handler that the material is in the DLB.

Ready to pick up signal.

This DLB is nothing more than the body of a plastic pen covered with similar covering to the bush. Perfect concealment

STEP THREE: ALL-CLEAR SIGNAL

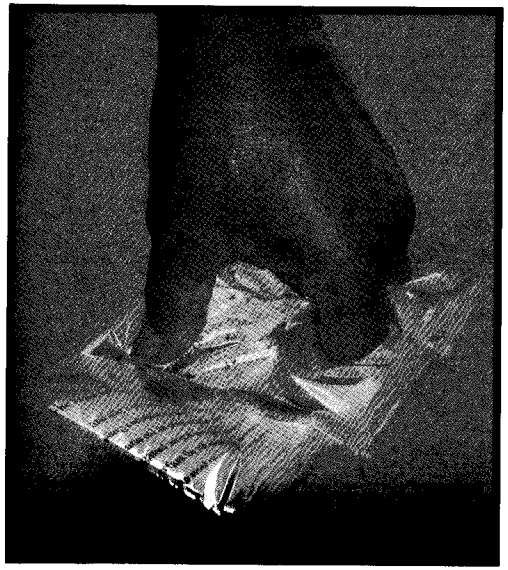
Only when the handler has seen the agent remove the ready-to-fill signal will he approach the DLB and collect the message. He will remove his own ready-to-pick-up signal the moment he has recovered the message. This tells the agent that he has recovered the message and that the DLB is now empty.

At this stage both the handler and the agent will leave the area. In the event that the handler has not shown up within the prearranged time, the agent will simply remove his ready-to-fill signal.

SECRETS OF DLB PLACEMENT

A spy will always remember that the aim of the DLB is to transfer information without the knowledge of any other person than the contact. The spy keeps these rules in mind:

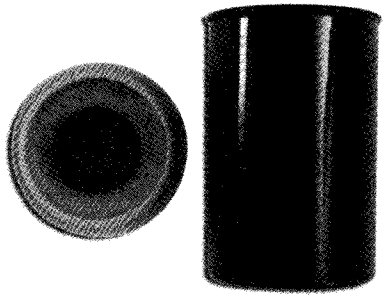
- He will always assume both himself and his contact are under surveillance
- He will create a DLB that fits in with his normal daily routine.
- He will make DLB placement and retrieval accessible and swift.
- He will be creative in his choice of container or hiding place.
- If he or his contact are apprehended, he will make sure the DLB cannot be discovered.



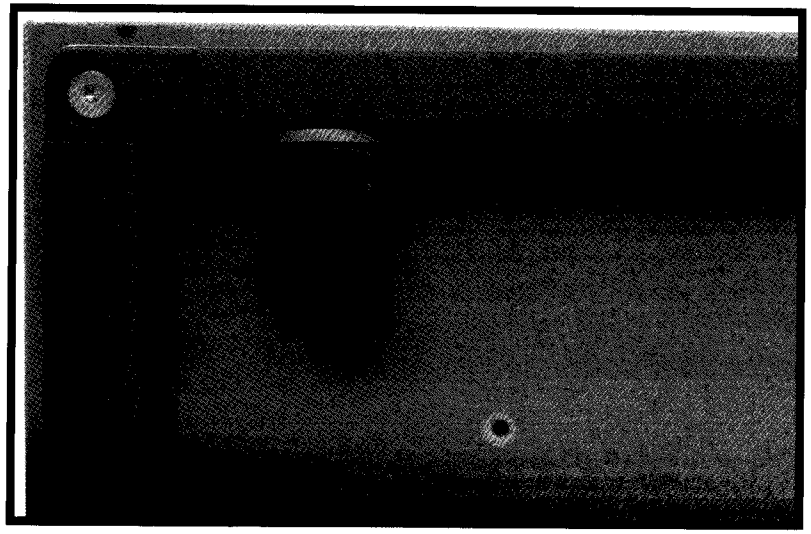
Although a message can be hidden underwater, the water should not be too murky and deep. Hiding the DLB is only half the problem – it has to be recovered quickly too.

USING A DLB

DLBs have purposely been made in the form of a hollow spike that has a screw top to make it waterproof. The message is simply put inside and then, at the right location, forced into the earth by standing on it. It is possible to construct a DLB from any form of tubing, but a better way is to use an old cigar case. This is almost perfect for the job, as it already has a waterproof screw top. Because the case is only made of light aluminium and can easily be crushed, the spy may disguise it as a twig instead of pushing it into the ground. He finds a stick of roughly the same thickness and removes the bark; he then uses this to cover the cigar tube. He then walks through the park holding it in his trouser pocket, making sure that the pocket has a hole in it and dropping his DLB at the required location.



Gluing a magnet inside a film container makes a quick and easy DLB. It can be attached to the metal underside of a table, chair or other household or office furniture.



CHAPTER 2

The art of writing and passing on secret messages is vital in a world where information means power.

SECRET CODES

There is evidence to suggest that coded messages were used as far back as Roman times. Codes and cryptology methods have been developed enormously since then, principally for use in military operations. For the most part, spies and agents were the first to use such codes and little has changed today.

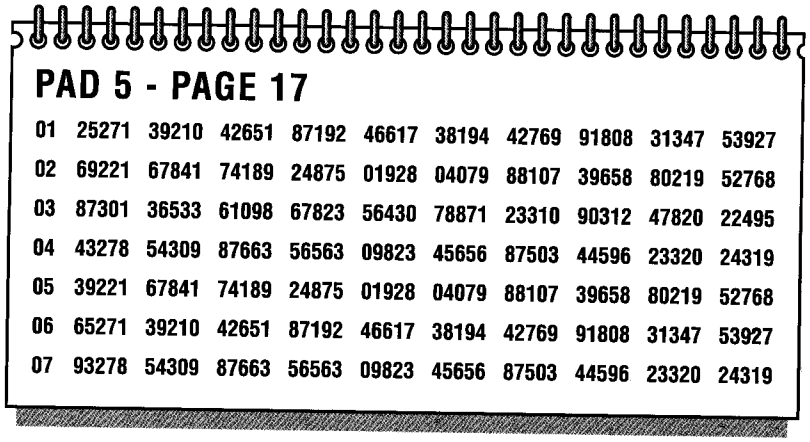
While messages can be passed covertly between the handler and the agent, there is always the possibility that the opposition might detect the exchange and intercept the message. To this end, all messages should be coded in one form or another. Many ingenious devices have been used over the years to enable governments, the military and spies to pass messages. One of the more widely known devices was the World War II German Enigma machine. Both Britain and America dispatched teams of agents in order to capture an Enigma unit so that they could learn its secrets and use any information they obtained to their advantage.

Despite its complexity, the Enigma machine's weakness lay in the fact that its code could be deciphered, even though this took an enormous effort. The main reason for this was simple; the coding and decoding procedure was a systematic and structured process. This meant that, no matter how complicated the system was, it could still be broken. In order for a coding system to be truly unbreakable, it must work in an unstructured way, in other words, randomly. The development of the One-Time Pad (OTP) went a long way to achieving this goal.

HOW TO USE ONE-TIME PADS (OTP)

A one-time pad, or OTP as it is generally known, is used for secret communications by just about all of the world's major intelligence agencies. Perfected in 1917 during the First World War, an OTP consists of random keys (number blocks) with the whole making a pad. These numbers are used only once, hence the name. OTP is the only cipher system that cannot be cracked. At the height of the Cold War, not a single OTP sent by the KGB was cracked by the American or British intelligence services.

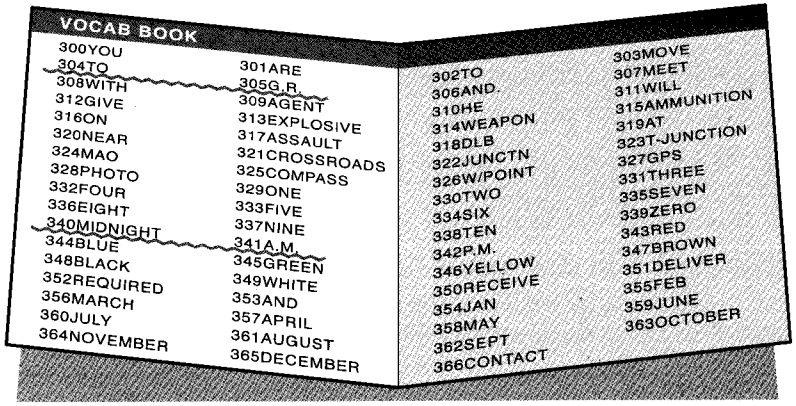
SAMPLE OTP



PAD 5 - PAGE 17

01	25271	39210	42651	87192	46617	38194	42769	91808	31347	53927
02	69221	67841	74189	24875	01928	04079	88107	39658	80219	52768
03	87301	36533	61098	67823	56430	78871	23310	90312	47820	22495
04	43278	54309	87663	56563	09823	45656	87503	44596	23320	24319
05	39221	67841	74189	24875	01928	04079	88107	39658	80219	52768
06	65271	39210	42651	87192	46617	38194	42769	91808	31347	53927
07	93278	54309	87663	56563	09823	45656	87503	44596	23320	24319

The above is a sample page from a one-time pad. The numbers are generated by random selection; the pad is numbered, as is the page and the line. There are only ever two copies of the OTP, one with the intelligence agency and the other with the field agent. The intelligence agency's copy is normally kept by the cipher operator, who works in a high security building, thus ensuring the safety of the copy. Very few people have access to the "pad", neither do they know which agent is using which pad. Only the ciphered message is passed up for intelligence analysis. The field agent will have the second copy. If he is compromised then he will destroy his pad in a special wallet that burns the pad in seconds. Even when the enemy has managed to get their hands on an agent's pad, there are simple checks that can be put in place to confirm authenticity. If the intelligence agency has the slightest suspicion that their agent has been compromised, they will automatically destroy their pad.



▲ **A sample vocab book**

There are many ways in which a numbered code can be deciphered into a simple language. This can either be achieved by starting at a random place in the alphabet triggered by a number or through the use of a common book, such as an encyclopaedia.

The most common form is to have a "vocab" book that lists a simple set of names and special letters and which will also provide the user with an alphabet from which he can spell place names that are not in the vocab book.

We can now translate the following massage using the vocab book above and then encrypt it using the OTP:

AGENT WILL MEET YOU AT GR327903 2 PM 5 AUGUST. HE WILL GIVE YOU WEAPONS AND AMMUNITION.

STEP ONE

Find the word "agent" in the vocab book and write down the three-digit number next to it, i.e. 309. Continue to do this until you have written down all of the digits. Any numbers in the message are simply left unchanged. You should finish up with the following line of numbers, which you should then separate into a block to match those in the codebook, in this example blocks of five:

30931 13073 00319 30532 79032 34253 61310 31131 23003 14306 31516

STEP TWO

Choose a line to start in your codebook, in this example we have used line three, and place the number block taken from the vocab book under those in the codebook. Next subtract without carrying units forward.

Black = codebook, blue = vocab book and red = the subtracted numbers.

87301 36533 61098 67823 56430 78871 23310 90312 47820 22495 43278

30931 13073 00319 30532 79032 34253 61310 31131 23003 14306 31516

57470 23560 61789 37391 87408 44628 62000 69281 24827 18191 12762

STEP THREE

Next add the codebook number, page and line to the front of the subtracted numbers i.e.

(51703) 57470 23560 61789 37391 87408 44628 62000 69281 24827 18191 12762

These numbers can now be safely transmitted to the agent; they will make absolutely no sense to an enemy unit even if they manage to intercept them.

STEP FOUR

Once the agent has received the message he uses the first block to identify the correct codebook, page and start line. (Agents may well have several different codebooks, using one for each person they deal with). The agent has the only other copy of the OTP code book, so it is a simple matter of placing the received message, less the indicator block, under the correct line and subtracting the numbers. The subtracted numbers are then broken down into blocks of three in order to find the message from the vocab book. Take the time to understand how the basic principles involved in OTP work. Once you have mastered the subtraction values, the rest is easy.

OTP CONSTRUCTION

Making your own OTP pad and vocab book is easy. Once completed, simply make one extra photocopy and give it to your contact. You can now exchange messages in total secrecy.

SPOT CODEBOOK

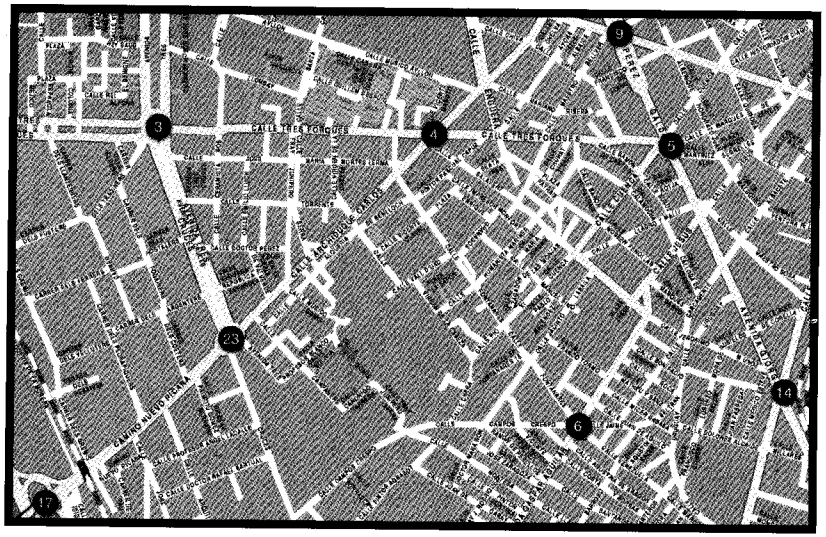
The spot code system can be used either by spies, agents or surveillance operators. It is a particularly good system as it allows the user to identify a major feature, usually a specific place, junction or crossroads. When a spot code system is used for surveillance, it allows the desk operator to know where all the surveillance operators are at all times. He can also direct foot and vehicle surveillance to a specified spot.

When used by handlers and agents, the spot code system offers several automatic back-up options. For example, if "blue 5" is compromised, both the handler and the agent will automatically know that they have to meet at "blue 6" and so on. This is how it works:

A SIMPLE SPOT CODE

A spot code is normally made by allocating a colour and a number to each major road intersection. As the surveillance operator drives from one intersection to another, he simply identifies himself and tells the desk operator. "Nine, this is Sierra Papa four – towards blue 5'30–35." When driving, the operator simply adds the approximate speed to the end of his call, providing a rough estimated time of arrival at the next spot. When the area is new to the operator, he will carry a spot codebook in his vehicle. However, should this codebook fall into enemy hands, it will present a short-term security risk. This will necessitate all the spot codes being changed and with everyone having to learn the new codes.

The spot code system can also be used to refer to actions rather than a location. This helps throw the enemy off balance should they be watching or listening to the operation. For example: "Sierra Papa four – towards black 6." In reality, the caller is simply telling the desk operator that he is static in one location, a cafe or a bar, for example.



MAKING A SPOT CODEBOOK

The spy may use a street map of his area, which can be easily and cheaply obtained from tourist offices or newsagents in the local area or even farther afield if he's exercising even more caution than usual. Any decent streetmap will do for his purposes. He will also buy some self-sticking coloured spot labels from an office supplies store. To make the spot codebook, he then sticks the spots at each of the major intersections and streets and number them. Then he will make a number of photocopies for each of his contacts, being careful to copy only the exact number of codebooks that he needs.

RANDOMIZE

A spy will use the coloured spots for one area but will make the numbers random. This will help confuse the enemy, but will make no difference to the agent.

INVISIBLE WRITING

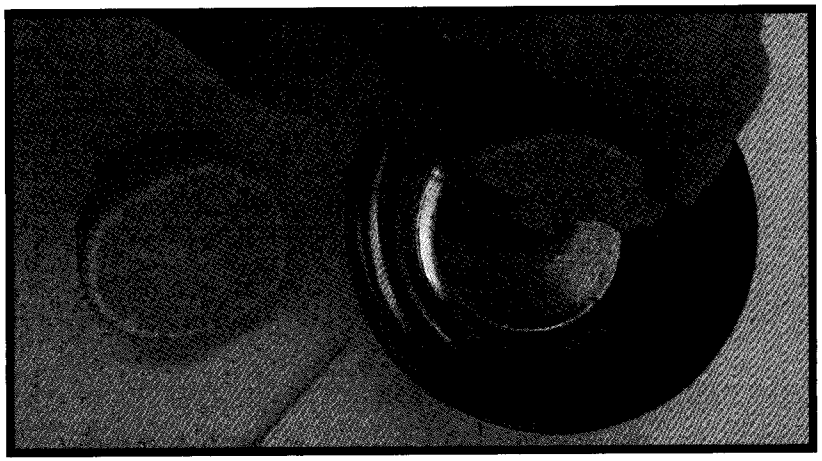
Writing invisible messages is also a good way of passing information between people; a message can be written on a bank note and passed quite naturally to another person. An agent or a handler may walk down

the street and discard an empty packet of cigarettes, a natural process, but the inner paper layer may well contain an invisible message. Despite having been around for centuries, the art of invisible writing is still widely used by many intelligence agencies today.

One of the problems with traditional invisible ink is that the author cannot see what they are writing. As a result, the message has to be short and very precisely written. Even when they were writing with an ultraviolet pen, the authors could not see what they were writing and the message could only be seen when the ink was highlighted with a special ultraviolet light.

Then, some years ago, the British intelligence service discovered, purely by accident, that a Pentel Rollerball makes a brilliant tool for invisible writing. The rollerball, commercially available in most parts of the world, writes normally on a piece of paper. The writing is then pressed against the piece of paper that will carry the secret message. The original ink dries almost immediately, so to the eye the message paper looks blank. However, when it is swabbed with a developing fluid, the message miraculously appears. It therefore allows the author to write a detailed and well-spaced letter in real time and transfer it to a blank piece of paper by what is known as "offset" printing. The transferred message will only become visible when it is developed.

MAKING INVISIBLE INK



▲ Any carbon-based clear liquid such as lemon juice or milk makes excellent invisible ink.

Any clear (not visible to the eye when dry), carbon-based liquid can be used to make invisible ink, milk and lemon juice being the most common. It is best to use normal writing or computer paper, as glossy or absorbent paper distorts the writing. Using an old-fashioned metal nib pen, although a toothpick would suffice, the spy will dip this into the milk or lemon juice and simply write his letter. The wetness provides some idea of he has written, but once the liquid is dry then the writing will disappear.

The best way to read the message is by using a domestic iron. The spy will run the hot iron over the paper. Because the liquid is carbon-based, it will turn brown and thus develop his message. Agents have used various forms of heat, such as gently moving the paper over a candle flame, in order to reveal the hidden message.

OTHER METHODS OF ENCODING AND DECODING MESSAGES

CODE WORD

The handler can make a list of code words that he can pass on to the agent; the list may be ten code words long and contain words where only one letter of the alphabet appears (no repeats) i.e. Blackstone. Blackstone may appear as number 4 on the list. The message may be hidden in a DLB or passed as a secret message. By a totally different signal, the handler will also indicate the list number, in this case number 4.

STEP ONE

The handler will write out the alphabet, next he will write down the code word followed by the rest of the alphabet omitting the letters in the codeword.

Plain text: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Code: B L A C K S T O N E D F G H I J M P Q R U V W X Y Z

STEP TWO

The handler will construct his message by taking the code letter below the normal alphabet letter. For example: I will meet you in the park. This will be translated as –

N WNFF GKKR YIU NH ROK JBPD – and then passed on to the agent.

STEP THREE

The agent, having received the numbers, checks the list for the number. The list may have been memorized to increase security further. The agent then writes out the alphabet, with the code word and the remaining alphabet written underneath. Using the encoded letters he will be able to decode the message.

ENCODING

If the message were to fall into enemy hands, regular blocks could help them decode the message. For example, the single letter N must either be an "I" or an "A". This can be avoided simply by dividing the encoded message into a four-letter block as shown below.

NWNF FGKK RYIU NHRO KJBPD

In the following message the code letter is PYROGENIC.

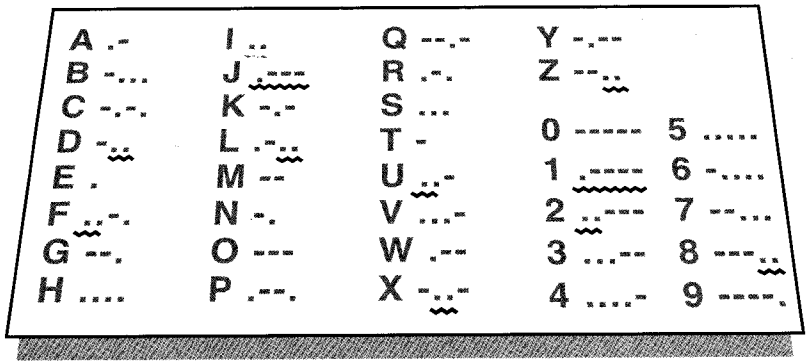
OGRJ OGOR JMMG RSDX

INGENIOUS CODES

Some of the codes that have developed over the centuries have been truly ingenious and, while these are rarely used today, it is worth looking at them. Although the best way of transcribing a message is to use the alphabet, the alphabetic and figure form can transcribe into symbols or sound blocks. While the best example of the latter is Morse code, many intelligence agencies have experimented with microwave and other sound devices.

MORSE CODE

Morse Code is just a simple substitution code based on dashes and dots. The dash is normally three times as long as the dot. The best way to define the difference is to repeat the words to yourself: "dot daaassh". Morse code can be sent in many forms, including radio, light flashes or acoustic sounds such as tapping on a water pipe.

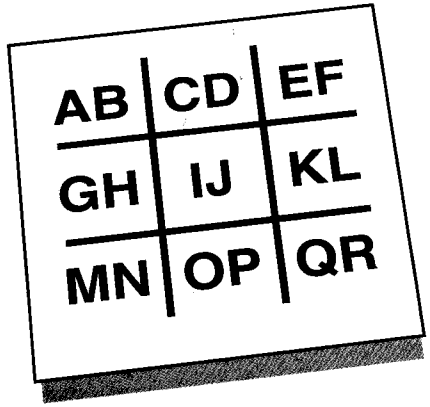


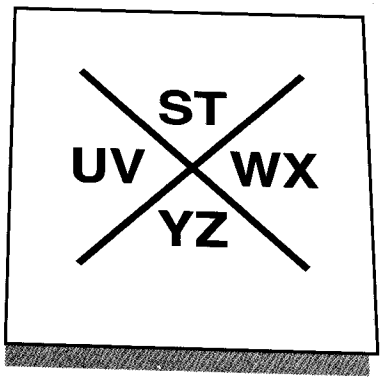
SYMBOL CODE

Many codes have taken the form of symbols. In biblical times, it was believed that the sign of the fish drawn in the sand was a sign of a believer in Jesus Christ. Symbolic writing can be complicated and can take years to decipher, as is the case with Egyptian hieroglyphics. A more down-to-earth symbolic code is "Pigpen". This uses a grid system designed in such a way as to allow two letters of the alphabet into each segment of the grid. The shape of the grid containing the letter forms the code.

STEP ONE

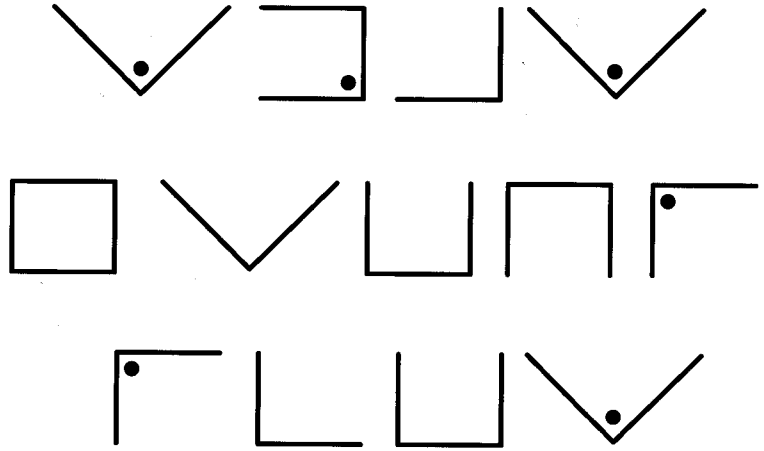
A grid is drawn in which all sectors are different. Then the alphabet is filled in; first in a logical order, i.e. AB in the top left-hand corner, following which they can be placed at random. If this is done, then both parties must know the sequence.





STEP TWO

The code is written using symbols, note that the second letter in each sector is denoted by a dot. The encoded message will look something like this. As with any encoded message, word block is best broken up into regular blocks to avoid the enemy decoding the message, should it fall into their hands.

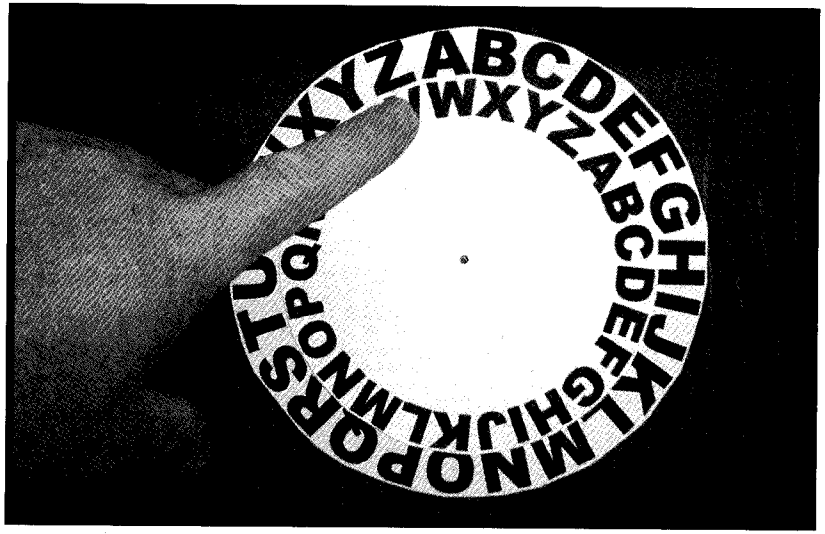


ENCODING AND DECODER RINGS

This a very simple substitution cipher, but one that can be used over and over while changing the code each time. Basically it uses two wheels, one that is about 1 cm smaller than the other. These wheels can be made of any material that can be written on. Around the outer edge of each wheel is the alphabet and the numbers 0 through to 9. The clock-face method is most commonly used to ensure that the writing is evenly spaced, so that the outer and inner markings are directly in line with each other. The idea is that the smaller disk can rotate inside the larger.

RING CONSTRUCTION

Two alphabetical and figure disks can be created using Microsoft Word. They are then printed out and stuck on to cardboard to ensure a more secure platform. Then they are pinned together in the middle so that the inner wheel rotates.



▲ Some simple cipher wheels.

STEP ONE

To encode a message, the spy simply turns the inner disk to wherever he wishes to start. He can rotate the inner disk until the A is now aligned with P. Using the outer disk as his plain text he writes down the aligned letter on the inner disk to form his code. The inner and outer circles need to be carefully aligned to read off.

STEP TWO

It is a simple matter of passing the code to the handler or agent together with the original start place on the outer disk; in this instance P. The matter can be made more complicated by having a more complicated start code, P7–V4–S6. To decode the message, he first places the inner disk at P and reads off the first seven letters. The inner disk will then be moved to V for the next four letters and to S for the remaining six. Decoded message should be kep in blocks.

COMPUTERS

There is nothing new about computer encryption. It uses the same cryptography methods that have been used for centuries. Few people, other than government intelligence agencies, had any need for cryptography prior to the digital age. That has all changed today. Businesses and individuals all generate information which, for one reason or another, they wish to

remain secret. The difference in normal human forms of cryptology and those developed for computers is simply one of security, i.e. it is easy for a computer to crack a human code, but not vice versa. Most computer encryption systems belong to one of two categories – symmetric-key encryption and public-key encryption.

Symmetric-key encryption is a secret code based on one individual computer. In order for one computer to send the encrypted message to another computer, the second computer must first know the same secret code. The secret code is the key to unlocking the information.

Example: In a simple form, a text-encoded message is sent to another computer telling the user that the secret code is 3. The encrypted process automatically changes the alphabetical information letters to 3 places down i.e. A becomes D and B becomes E etc.

This is a very simple explanation of how computer encryption works, but it should be stated that today's encryption systems are highly advanced.

Public-key encryption uses both a private key and a public key. Whereas only your computer knows the private key, any other computer that wants secure communications can access your computer's public key. In order to decode the incoming message, the receiving computer must have and use both the public and the private keys.

PASSWORD PROTECTION

Secret data can be sent by computer by using the "Options" button found in the "Tools" file of Microsoft Word. The spy will be asked for a password in the "Security" box. (On a Mac, the procedure is via "Protect Document" in "Tools"). The password has to be reconfirmed but the document is then secure as the recipient cannot open it without knowing what the original password is.

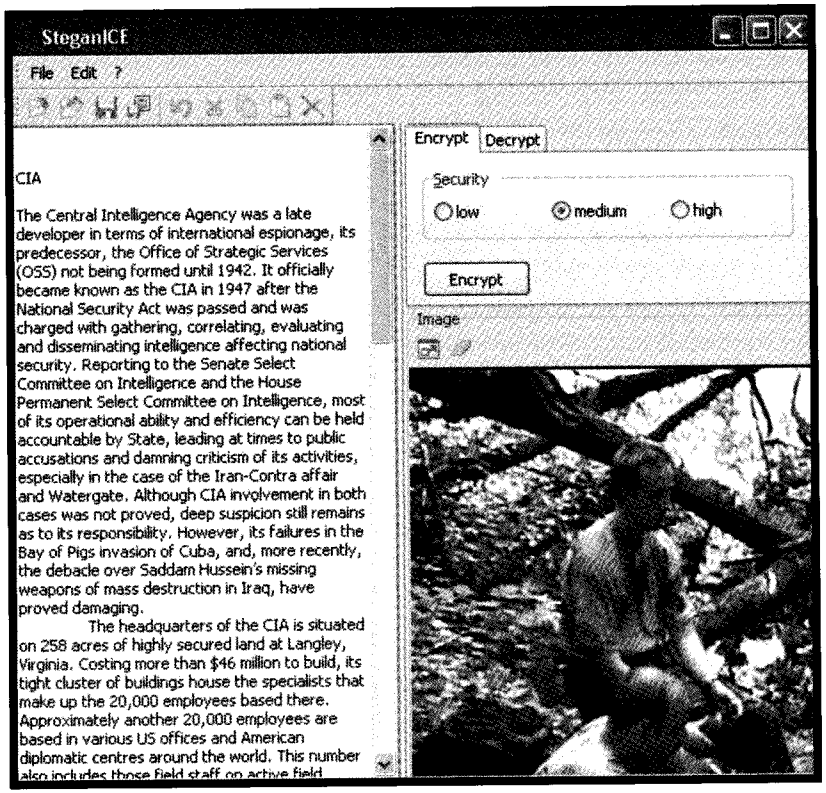
A spy will change his password regularly.

HIDING A TEXT FILE IN A DIGITAL PICTURE

One way of sending secret messages is to hide confidential data in inconspicuous graphic files. This file is then sent to a contact over the Internet or on a disk. With the appropriate software and code word, the text can be taken out of the picture. One such system uses the well-known steganography technology that is also used for digitally watermarking pictures. Bitmap graphics consist of pixels that can be modified to store your text. If the altered picture – containing the text file – is then seen by someone else, it will simply look like a normal image. It works by removing or altering some of the bits that make up the picture pixels and replacing them with the text. To the human eye these changes cannot be seen as only insignificant information is removed and this is done across the whole spectrum of the digital image.

One of the best shareware programmes for hiding text inside pictures is called StegenICE and a free download can be found at the following address:

http://madmax.deny.de/siteJS/indexJS.htm



▲ Hiding text in a picture is a modern, hi-tech way to conceal a message.

CHAPTER 3

We are all being watched, listened to, and recorded – all of the time.

SURVEILLANCE

There are many forms of surveillance but, for the most part, people believe that they can go about their everyday lives expecting a certain amount of privacy – this is not true. Every single person in Europe is under some form of surveillance every day. They will not deliberately be observed or overheard, but records of their movements and actions will be recorded. Close Circuit Television (CCTV) cameras currently monitor city centres, major stores, petrol stations and motorways. Credit card transactions can be traced. Your emails can be read, as can every stroke of the keyboard. And then there is Echelon...

ECHELON

Echelon is the name given to the massive worldwide surveillance system that is capable of capturing and scanning every telephone call, fax and email sent anywhere in the world. Using sophisticated satellite systems, earth stations, radar and communication networks, as well as an array of ships and planes, the system is capable of monitoring both military and civilian communications. It was originally developed during the Cold War by the English-speaking countries to eavesdrop on communications between the Soviet Union and its allies. Now that need is no longer pressing, it is being used instead to monitor terrorist communications, as well as the activities of organized crime groups, alongside more traditional espionage methods.

Although details about the system are still shrouded in secrecy, some facts are known. The main proponents are the US and the UK, but they are backed up by Canada, Australia and New Zealand. Each country is responsible for monitoring a certain part of the Earth. For example, the US listens in over most of Latin America, Asia, Asiatic Russia and northern China. Britain monitors Europe, Africa and Russia west of the Urals. Canada sweeps the northern parts of the former USSR and the Arctic regions. Australia is responsible for Indochina, Indonesia and southern China and New Zealand handles the western Pacific.

In practice, the way Echelon works is simple. All the members of the alliance use satellites, ground receiving stations and electronic intercepts that enable them to pick up all communications traffic sent by satellite, cellular, microwave and fibre-optic means. The communications captured by these methods are then sent to a series of supercomputers that are programmed to recognize predetermined phrases, addresses, words or known voice patterns. Anything deemed to be of interest is then sent to the relevant intelligence agency for analysis.

In the US, the agency responsible for Echelon is the National Security Agency (NSA), based at Fort Meade, near Washington. It is estimated that both its staff and resources exceed those of the combined CIA and FBI. Canada's Echelon program is handled by the Communications Security Establishment, an offshoot of the National Security Agency, and is based in Ottawa. In Britain, General Communications Headquarters (GCHQ) located at Cheltenham, is concerned with Echelon. You have to remember that the locations of smaller stations are spread across the globe in strategic positions.

After the Cold War and before 9/11, the US primarily used Echelon as a means of intercepting messages from South and Central America in an effort to thwart drugs barons. Other organized crime gangs and terrorists, such as the Russian Mafia and Hamas, were also a target. However, following 9/11, it must now be assumed that Echelon is on the alert for any messages that might warn of an attack by Al Quaeda.

Although such usage of a surveillance system can only be a positive thing, Echelon has also had its fair share of detractors. Certain accusations have been made that Echelon has been used for commercial gain by the countries involved, enabling them to undercut competitors and to double deal to their own national economic advantage. Debates have even been raised in non-participating countries and within the EU. Nevertheless, the

intelligence gains provided by the system in the new climate of global terrorism are likely to drown out any protests in the future.

WHAT IS SURVEILLANCE?

Surveillance is a technique used to obtain information, to make connections, to produce new leads and to collate evidence. Surveillance can be carried out by one of the following methods.

- Human, visual and audio.
- Electronic, video and audio.
- Aerial and satellite surveillance.

Surveillance may be carried out in order to obtain evidence of a crime or to identify persons who have been indicated in subversive actions. Surveillance methods help to establish a person's location and may well lead to an association with other criminals. The location of stolen or contraband goods can be exposed, leading to an admissible case in court. However, the main way that surveillance is used is to gather military intelligence. Governments have long since learned that information gathered on the potential lethality and capabilities of another nation can help them prepare for defence or attack. One good example is acoustic intelligence. This is derived from monitoring the sounds made by enemy surface vessels and submarines. These sounds can be analyzed to provide a unique signature for each vessel currently at sea. Knowing the location of enemy nuclear submarines or battle fleets provides advance warning of any attack.

One major problem with military intelligence is the amount of information they collect. Having information is one thing, interpreting its full and true value is quite another. The enormity of this quandary was highlighted by the 9/11 Al Quaeda attacks on the United States. The information that an assault was about to take place was available from several sources: the interpretation and immediate action lagged too far behind. Echelon should have detected some traffic. Or do the perpetrators of the atrocity have a method of sending messages that cannot be detected? Whatever the reason, it proves that electronic surveillance, no matter how sophisticated, is only effective if it has the back-up of good analysis and the correct distribution of intelligence.

In reality, surveillance is simply monitoring the activity of a person or persons, a place or an object. In order to do this successfully, intelligence agents need to consider several factors about the target. For example, if the target is a person then he will most probably move around, either on foot or by vehicle. If the target is in a house in the country, a static observation position (OP) would be set up. Note that following people and surveillance is undertaken by spies and it is usually illegal. Civilians and members of the public should not do it. The various methods of surveillance consist of one or a combination of the following:

- Static surveillance.
- Foot surveillance.
- Mobile surveillance.
- Technical surveillance.

SURVEILLANCE OPERATOR

◂ A surveillance operator.

A good surveillance operator is known as a "grey" person. That is to say that they mingle with people, but that no one ever takes any notice of them. Their personality appears nondescript. They have no outstanding physical features and their dress is innocuous. They are deliberately trained to be Mr and Mrs Nobody, so insignificant that no one ever gives them a second glance.

Yet this is only an outward appearance, as the surveillance operator requires many skills. They must be patient, as surveillance operations can go on for months, sometimes even years. They must be adaptable, as many targets can act erratically. If the target is a professional spy, they will

deliberately check to see if they are being followed and will take evasive actions in order to throw off any unseen surveillance operation being carried out against them.

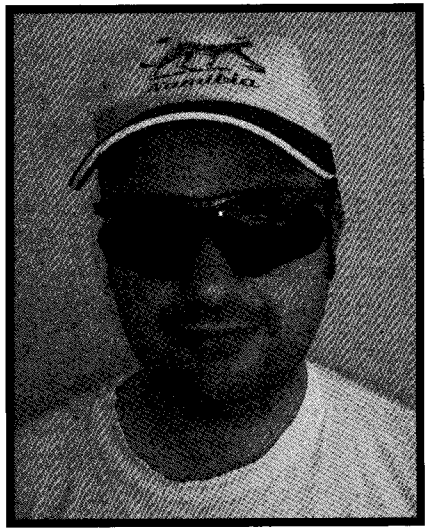
Surveillance operators must have confidence not only in their own abilities but also in those of their team members. They must have a good memory, good hearing and excellent eyesight. Most of all, though, surveillance operators must blend into the background and become almost invisible. If the target takes a bus, one of the team must follow. The target will observe anyone who entered the bus at the same stop and be aware that they may be surveillance operators. In this situation, the surveillance operator becomes an actor, conversing with the passenger next to him as if they have known each other for years. The target may even approach the surveillance operator and deliberately confront him as to why they are being followed. In this instance, the operator must deliver a response that satisfies the target's inquisition.

The surveillance operator must also learn advanced driving skills and be able to operate any number of different vehicles. Most surveillance operators in the United Kingdom undertake a high-speed driving course with the police. This involves handling a vehicle at speed. They must also have a good knowledge of the area in which they are working. This is particularly helpful when a target has become temporally "unsighted". Above all, they must possess and develop a "sixth sense" – something that comes with good training and experience.

Some surveillance operators specialize in technical surveillance. They must learn how to use and operate a whole myriad of technical equipment, such as cameras and listening devices. In many cases this means covertly breaking into someone's property and inserting an audio-visual device. To do this successfully surveillance operators are required to learn method of entry skills, such as lock picking. Other operations may require them to crawl beneath a vehicle during the hours of darkness and insert a tracking device.

It is important for the surveillance operator to understand who or what the target is. If the target is a person, he needs to ask himself whether that person is aware that they may be under surveillance. If the target is a foreign spy, then he will have been trained in counter-surveillance methods. Even if the target is a common criminal, he may, due to the nature of his activities, become suspicious of being followed. In many cases, a surveillance target may not be aware that he is being watched or followed, or he may have been getting away with his activities for so long that he has become complacent. Knowing these factors helps the surveillance team decide on the number of people required and what approach they should take. Likewise, where the target is a static location, such as a building, it is important for the surveillance operators to evaluate what resources are needed.

MASTER OF DISGUISE



◂ Disguise should be subtle.

There may be times when a spy or agent is required to become a master of disguise. He may suspect that he is under surveillance and wish to throw his pursuers off in order to make an important meeting, for example. Or he simply may want to go somewhere to observe someone or something and not be recognized. Whatever the reason, there are two basic methods: the immediate quick change and the deliberate disguise.

A quick change requires some thorough and prior preparation. For instance, it is possible to change his stature, dress or appearance or a combination of all three. Stature can be addressed by stooping, limping, effecting a height change or body bulk size. Changing his dress requires conversion or having an alternative item of clothing with him. Likewise his appearance can be changed in a few minutes if he is prepared. The basic rule is to start off as Mr Average and change into Mr Nondescript.

The spy will remember that it is easier to dress down than it is to dress up – by the same token it is easier to look older than it is to try to look

younger. All these tricks can be done on the move, but they are best performed while temporarily out of sight, such as in a crowded pub toilet. Changing his ethnic appearance is a good ploy to use at night or during foul weather. The spy will make use of the following tricks:

- Placing a stone in his sock to create a realistic limp.
- Making himself look taller by adding rigid foam pads to his shoes.
- Wearing a cap. When he removes it, he looks shorter.
- Placing half a folded newspaper on each shoulder to make his waist look thinner.
- Putting cotton wool in his mouth to swell out his cheeks.
- Putting on or removing glasses.
- Burning a cork and blackening his face where he normally shaves – to imitate stubble.
- Using soot, burnt paper, talcum powder or cigarette ash to change his hair colour.
- Carrying a dark brown shoeshine sponge, so that he can totally cover his face, neck and hands.
- Carrying items in his pockets, such as a carry bag, fold-up walking stick, cigarettes, baseball cap or a plastic raincoat.

A deliberate disguise is a more planned affair, but the same basic tactics apply. If the reason for disguise is for the spy to go somewhere and not look out of place, he will undertake a recce of the area to pick up ideas. The spy will never be inclined to dress to bring attention upon themselves. If the area is busy with tourists, or students for example, he will dress accordingly.

SURVEILLANCE VOICE PROCEDURE

Vehicle surveillance operators must learn some basic codes and a jargon that, while being slick and brief, is clear enough for all personnel to understand. There are several reasons for doing this; firstly it helps identify who is doing what and where a particular surveillance vehicle is in relation to the others. Secondly, it helps to minimize the amount of voice traffic over the radio.

One such code, popular with surveillance teams, is the phonetic alphabet. It can be used to identify targets, vehicles, operators and places. Numbers are added to enlarge and identify various units, for example, vehicle SP4 would be spoken as "Sierra Papa Four" and be part of a Special Patrol surveillance team.

WHO'S LISTENING?

While covert radio conversations are secure and cannot be listened to by any third party, the fact that a vehicle is transmitting something can be detected. In many cities, especially where the district is controlled by terrorist organizations, it would be practical to assume that they have a monitoring capability. This is usually found in the form of "watchers", young men or women who stand on the street corners with a handheld device that indicates that a vehicle is transmitting on a secure frequency. Of course, this helps the enemy identify possible surveillance vehicles.

THE PHONETIC ALPHABET

▸	A	Alpha	▸	N	November
▸	B	Bravo	▸	O	Oscar
▸	C	Charlie	▸	P	Papa
▸	D	Delta	▸	Q	Quebec
▸	E	Echo	▸	R	Romeo
▸	F	Foxtrot	▸	S	Sierra
▸	G	Golf	▸	T	Tango
▸	H	Hotel	▸	U	Uniform
▸	I	India	▸	V	Victor
▸	J	Juliet	▸	W	Whisky
▸	K	Kilo	▸	X	X-ray
▸	L	Lima	▸	Y	Yankee
▸	M	Mike	▸	Z	Zulu

Surveillance operators also use other terminologies to indicate a number of actions the target vehicle is likely to carry out. This terminology also helps the surveillance team keep the target vehicle within sight and thus avoid a lost contact. While they vary from country to country, here are a few examples of vehicle surveillance terminology with an explanation as to what each means.

TYPICAL TERMINOLOGY USED BY VEHICLE SURVEILLANCE TEAMS

"Back-up, can you?"	Eyeball request to back-up vehicle to ascertain whether a handover is appropriate. Response is either "Yes, yes", "No, no" or "Back-up can at next junction".
"Back-up"	The second vehicle in the convoy.
"Cancel"	Ignore the instruction or information just given.
"Come through."	Given after "hang back" to bring the convoy through.
"Committed."	The target vehicle is committed to travelling on the motorway.
"Contact, contact."	The eyeball has been regained by one of the vehicles in the convoy, following the search procedure. The pick-up vehicle will also give a location.
"Convoy check."	Request from eyeball to determine position of vehicles in convoy, to which all vehicles automatically respond in turn. Motorcyclists should respond without specifying their precise position, after Tail-End Charlie has reported. When all correct, eyeball calls "convoy complete".
"Down to you."	The final transmission made by eyeball before handing over surveillance to another vehicle.
"Eyeball regained."	The target vehicle is once more under surveillance.
Eyeball.	The vehicle or officer that has primary visual contact with the target and that is directing the operation for the time being.
"Footman out."	A vehicle in the convoy has put an officer out on foot.
"Going round."	The target vehicle is commencing a second or subsequent circuit of the roundabout.
"Hang back."	Transmission from eyeball, indicating that the convoy should hold back as the target is slowing down or has stopped.
"Held."	The target has made a temporary stop. This will normally be followed by an explanation for the stop, i.e. traffic lights, pedestrian crossing, traffic congestion etc.
"Left, left, left."	The target vehicle has turned left. In some cases, such as on a motorway, the junction number may be added, i.e. "left, left, left 57".
"Manoeuvering."	Warning issued by eyeball, indicating that target is, for example, manoeuvering on the forecourt of a garage, business premises, car park etc.
Nearside, offside.	Indicates that the nearside/offside traffic indicator is active on the target vehicle.
"No change."	The situation remains unaltered.
"No deviation."	The target vehicle is continuing straight ahead, as at a crossroads. It is said to reassure the team that there has been no change of direction.
"Not one, not two."	The target vehicle negotiating a roundabout has passed first, second exits etc.
"Off, off, off."	Transmission by the eyeball, indicating that the target is now on the move.
"Original, original."	The target has resumed after a stop, in the same direction of travel as before.
"Out, out, out."	Transmission by the eyeball, indicating that the target is alighting from a vehicle or that he is leaving a premises.
"Reciprocal, reciprocal."	The target vehicle has done a U-turn and is now returning along the same route.
"Right, right, right."	The target vehicle has turned right.
"Roundabout, roundabout."	The target is approaching a traffic roundabout where he has a multiple choice of exits.