EXTRACTS FROM EYE SPY INTELLIGENCE MAGAZINE

** images are presented in low-res screen shots for quicker loading*

SECRETS OF THE SPIES

Tradecraft: From installing bugs to the art of 'going grey'. Major Eye Spy features focusing on some of the most important traits of a spy and issues affecting those who work in the intelligence business.

TITLE: THE ART OF GOING GREY

SUB TITLE: THE TRADECRAFT THAT ENABLES SPIES TO PERFORM WITH NEAR IMPUNITY

ISSUE 37

In the UK there is a clear distinction between an intelligence officer and agent. An officer is usually an official on the payroll of government and, if working overseas, he or she is probably attached to an embassy or in the employment of a registered company. An agent can be anyone prepared to pass on useful information, be it a simple tip or high-grade intelligence, or he can be hired, trained and given guidance on how to obtain it. The agent is paid by the state via his controller or handler, but don't expect to find a wage slip. This description varies from country to country; some nations describe intelligence officers as 'agents', though for the purposes of this Tradecraft feature we have used the British model. A powerful feature that covers fully the 'art of going grey'.

As an added bonus, both MI6's spy training facility - ***'THE FORT'*** *and the CIA's* ***'THE FARM'*** *are covered.*

EXTRACT

OCCUPATION OR ROLE

Most spies are employed in a job or environment whereby intelligence can be gleaned or is specifically required. When travelling abroad, just like business persons or holidaymakers, counter-intelligence begins at the airport or border crossing. "What is the nature of your business?" is probably the most common question asked by customs. Give a wrong answer and the operation could be compromised before it has begun. An experienced officer and agent will prepare - check every detail, from examining his vehicle for broken lights, or making sure a credit charge card has sufficient funds. A convincing cover story is absolutely essential, and most operatives put in place a telephone number whereby a credible business associate or company can validate the story.

CLOTHING AND APPEARANCE

It seems bizarre that in these days of heightened tension and uncertainty, political correctness even applies to the world of espionage. Just a few months ago, two undercover SAS surveillance officers were challenged in Iraq and their subsequent arrest resulted in a major incident. Both men were in a vehicle and wore local attire, yet they were betrayed by standard British Army boots. 'Blending' in to any environment is by any definition crucial and most agents will reconnoitre their area of operations. Unfortunately, terrorists have learned this spy trait as well.

Clothing: It is crucial for any operative or undercover agent to don the correct attire. It is inconceivable and inappropriate to wear clothes, hats or sport unusual haircuts. The wearing of jewellery, designer clothing or even a distinctive tattoo or earring could attract undue attention...

LOCATION AND LANGUAGES

When operating undercover, especially abroad, language is vitally important. If commissioned to gather intelligence overseas, learning dialect and understanding traditional local behaviours is very important. Some intelligence services avoid the subject of 'perfect speech' by providing officers with a manufactured past, i.e., an auntie or relative living in a foreign land: you spent your "early years abroad" - hence the dialect. Voice techniques and education are important and regional variations in language and culture must be taken into account. A good excuse for being in an environment often quells inquisitive minds, therefore research in this area is essential.

Officers and agents are often chosen for specific tasks, and it is unlikely a pupil educated in Oxford speaking the 'Queen's English' would be assigned to a task in a remote mining town in Russia. **Selection** is of paramount importance. The use and 'turning' of locals in foreign lands is a skill....

TITLE: SECRETS OF THE SPY TRADE 1

SUB TITLE: THE SWITCH OR LIVE DROP
ISSUE 26

The art of intelligence gathering has changed dramatically as emerging technology affords the 'spy' with many new avenues of acquiring secrets. However, computers and modern 'gadgets' will never replace some of the 'established' trade secrets - such as holding your nerve, or in this feature - exchanging information in a subtle, but covert manner. Eye Spy takes a candid look at a few tricks of the trade...

Hiding a package or message for a colleague or acquaintance to locate is not a difficult task. First you have to find a suitable location that is discreet and known to both parties. This is often referred to as a **'Dead Letter Drop'** or 'Box' or 'DLD'. Sometimes it is not possible to prepare for such an exchange, and persons must meet face-to-face. This is called a **'Live Drop.'** Get it wrong, and it could cost you more than the contents of the packet.

Changing hands: The book drop - switch and exchange

BRIEFCASE SWITCH

A typical switch may involve strolling through a leafy park and sitting on a park bench. Placing the briefcase on the floor and lighting a cigarette or reading a book is a natural delaying tactic. Along comes another person carrying an identical briefcase and sits next to the first person - placing *his* case alongside the other one. A few moments pass before the second man lifts the first briefcase and walks away. The scenario is simple and effective. But there are many variants to 'The Switch' which are better performed in populated areas, buildings, or even crowded elevators. If performed well - a surveillance officer will find it difficult to spot.

The simplest way of passing a message or item to a person is called the **'Brush Pass', 'Reverse Pickpocket'** or **'Handover'**...

Eye Spy looks at a multitude of variants involving this simple, but effective tradecraft, including the 'Lovers Switch' - a kiss over a candlelit table or departing train - the package is slipped carefully into the mouth.

TITLE: SECRETS OF THE SPY TRADE 2

SUB TITLE: DEAD LETTER DROPS
ISSUE 27

It was during the Cold War that counterespionage officers first coined the term 'dead drop' or 'dead letter box'. However, this fascinating area of espionage has been used for thousands of years and is truly global. But finding a secure location for the covert exchange of information, equipment or money is not as easy as it seems.

Eye Spy takes a look at some of the skills and traits required to make the perfect drop...

Establishing locations for dead drops takes time and is often dependant on the type of material being handled. For example, it is of little use using a tiny hole in a wall if two persons are intending to engineer a deal involving a box containing weapons or a significantly over-sized package.

Agents will often establish a number of drop zones and provide each with a designated name or code. Dead drops are relatively obscured from public view, though not always. It has been known for public telephone boxes, garbage bins and even lamp posts to be used in the middle of a high street.

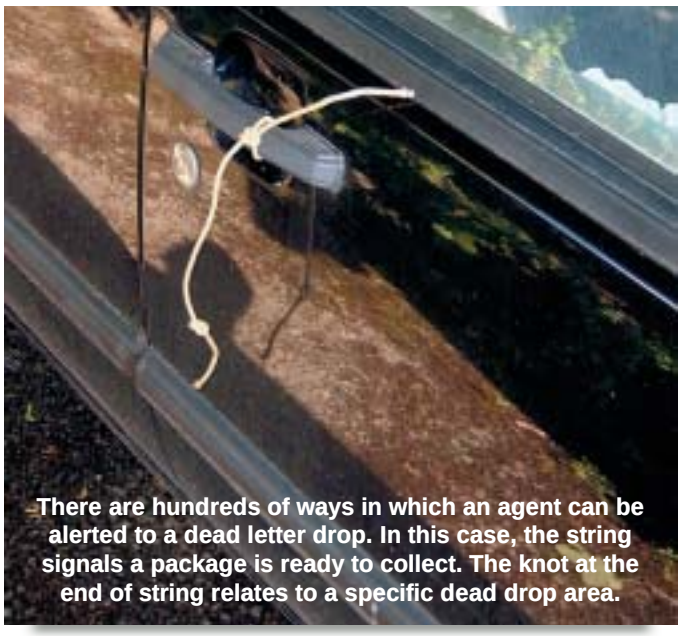
Brompton Oratory in Kensington, London. The KGB used this location to pass on and receive intelligence during the Cold War

The locations chosen for a drop are usually on public land. Select a location on private land or in secure premises means the risk of exposure increases dramatically. Police or security guards would become suspicious of any stranger wandering through a garden or private car park in the middle of the night, for example.

The ideal location is a place where people congregate or pass through everyday. A bus or train station, a shopping mall, wooded parkland, reference libraries, churches, public buildings. Again, all of these places are dependant on the type of exchange. Even as a frequent visitor, the chance of anyone becoming suspicious is about zero.

ASSESSING THE LOCATION

If the operative requires only to leave a written item, a library is ideal. Shelves are packed with books, and provided the agent does not choose a popular work, then leaving a message in a book is quite safe....



There are hundreds of ways in which an agent can be alerted to a dead letter drop. In this case, the string signals a package is ready to collect. The knot at the end of string relates to a specific dead drop area.

TITLE: ORIGINS OF THE BRUSH PASS

SUB TITLE:
ISSUE 29

Author Benjamin Weiser, in his notable book, 'A Spy's Life', which focuses on the remarkable story of Ryszard Kuklinski, a Polish officer who passed on huge amounts of intelligence about the USSR to the United States, also researched some fascinating techniques in espionage operations. One of the tricks developed in that era - a period plagued with spies and tension between the superpowers - involved the 'brush pass' or 'brush contact'.

The origins of the 'brush pass' can be traced back to America and the CIA, and involved the skilful manipulation of gaps in surveillance and the covert passing of items from one person to another without being noticed... even if the exchange is under observance.

EXTRACT:

Smith had another inspiration. One of his students was a Czech intelligence official who had volunteered to work for the United States and was receiving tradecraft lessons in New York before he was sent back to Prague. One evening at rush hour, they were at Grand Central Terminal in midtown Manhattan. Smith was training the agent in the use of signals and dead drops, but it was clear that the agent was reluctant to leave a package unattended for any length of time. "Anything I put down for you is going to incriminate me, and anything you put down for me is going to have stuff that will incriminate me," the agent said.

Smith replied, "Your concern is that it's sitting out there with nobody in charge?" The agent nodded. Improvising, Smith escorted the agent to a subway entrance near Grand Central, which also led into the old Biltmore Hotel. A pedestrian could walk straight into the hotel or turn right and descend a flight of steps into the subway. "Let's try this," Smith said. He asked the agent to stand inside the crowded doorway at the top of the stairs leading down to the subway, where he could not be seen from the street. "I'll walk through the door, and hand you a newspaper," Smith said. "When you get that newspaper, turn around and go down the stairs, and I'll go straight into the hotel."

TITLE: SPYING

SUB TITLE: NEW TECHNIQUES FOR AN OLD PROFESSION
ISSUE 24

The planting of secret surveillance devices still happens, of course, but the word 'bug' now has many applications. Eye Spy Associate Editor Glenmore Tranear-Harvey explains why it's almost impossible to guard against today's 'super bugs'

You don't have to be a terrorist, international drugs-smuggler, money-launderer, intelligence officer from a hostile country - or even Koffi Annan - to be the object of covert surveillance by the clandestine services. The world of espionage embraces us all. As you go about your daily life, you could be the subject of eavesdropping and surveillance. (So, benefit cheats, illegal immigrants and errant husbands beware!)

The modern day 'spook' has a wide range of techniques and top-secret gadgetry available. You can be spied upon in practically every situation. It doesn't matter whether you are in the 'privacy' of your home or office; whether you are walking or in a car; in a crowded party or in the middle of a field; in daylight or with the 'cover' of darkness. Your every word, movement or action can be detected and recorded by the security and intelligence services.

Let's consider some:

Thinking of popping that sensitive letter in the post? Secret equipment enables your mail to be scanned and read without the envelope seal being opened.

So what about email, faxes or the internet? Anything you send using digital transmission can be 'tracked and cracked'. Even encrypted or 'hidden' messages. Steganographic scanners can detect the electronic equivalent of a microdot, by isolating individual pixels buried in an internet website image. Your computer can be 'hacked' so that all of your computer's contents can be viewed remotely at any time by the 'watchers'....

TITLE: BUGS AND EAVESDROPPING

SUB TITLE: NOTES ON WIRE-TAPS, TARGETS AND COUNTERSURVEILLANCE
ISSUE 41

According to senior counter-espionage and counter-terrorism officers, phone tapping and bugging is a valuable intelligence tool. Most law-abiding citizens believe evidence acquired covertly, including from phone taps, should be used more freely and openly in court. Several civil liberties' groups are opposed to many aspects of government bugging, and many are opposed to covertly recorded conversations being heard in court. A major intelligence concern is that crucial techniques used by the security services to perform such tasks will be exposed. However, many methods used by surveillance officers, including bugging, are already well known. Only compromise or the discovery of bugs by those under observance is problematic, according to undercover agents interviewed by Eye Spy.

In this fascinating overview, Eye Spy examines many aspects of bugging, undercover work and countermeasures. It also covers:

- Who uses listening devices?
- Phone tapping
- Visual and audio bugs

A US government surveillance officer takes a cautious peek inside a house already under investigation. Prior to any bugging operation, experienced officers will spend time examining the layout and surrounding area. It is vital that their actions go undetected at this stage. 'Trade secrets' are heavily protected, but officers have built-up volumes of information that will help in any kind of environment. Despite this, operations are often dictated by time, finance, man-power and urgency. In many cases, the first time the media or public will learn of an investigation, is via a police statement. Only then will journalists realise MI5 or FBI specialist officers must have been deployed

- Trade secrets
- Recording without a recognised bug
- Car tracking devices
- Bugging meeting rooms
- Using the 'wrong number' trick
- Surreptitious entry
- Cell phone bugging
- Defeating 'safe houses'
- Choosing the right equipment
- Identifying countermeasures


A typical land-line telephone bug

EXTRACT:

DEFINING THE INTELLIGENCE

To ascertain the correct equipment to use, government officers will first access the situation, environment, and above all, note what the goal of the operation is. If all that is required is the name of a drug dealer operating on a housing estate, for example, the best option is to use an **informant.** A 'ready made' list of targets is quickly available for further action. If no informant is forthcoming, undercover officers will have to use other methods to gather intelligence - that usually means posing as a *buyer* or *seller.* A simple **body-worn** microphone/transmitter is quite useful, though risky in many circumstances. If discovered, the agent is in danger. However, a transmitter can glean vital information that is immediately relayed to other officers in near proximity. If they sense danger, they can react quickly. Similarly, agents usually use **code-words** to reflect how the conversation or meeting is progressing. A **'trigger'** word warning that the meeting is deteriorating, or that assistance is required, is always decided upon *prior to* any undercover operation...

EXTRACT:

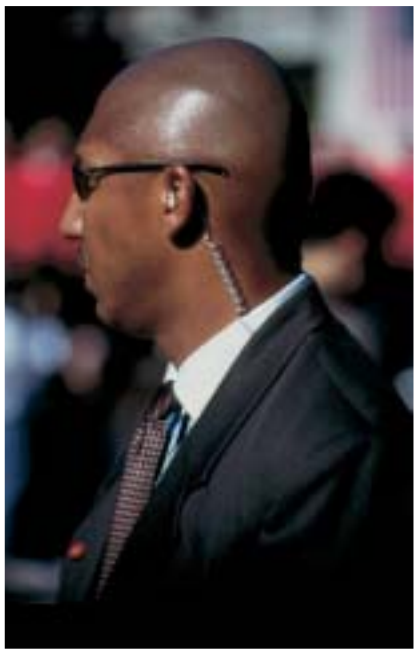
PHONE TAPPING

Legal phone tapping can only be conducted in the UK, USA and Europe after the issuing of a court warrant. Intercepting incoming and outgoing phone calls, in most cases, is via a telephone exchange. The security services can then identify the number of the caller and receiver. Rarely do undercover officers actually place a bug on the line, in the phone or handset - however it does happen. Unlicensed operators can also use similar technology in the form of devices that simply clip on the telephone line and transmit the conversation to a receiver. Unfortunately this takes only about 10-15 seconds, and the clip is usually placed on a section of line that is hidden from view - in the undergrowth or behind a fall pipe.

TITLE: TRADE SECRETS

SUB TITLE: HARD PINS - CRESTS, INSIGNIA AND SECRET IDENTIFICATION

ISSUE 14



Planning for the arrival of a dignitary or VIP is essential. In the world of intelligence it can be crucial.

Government close protection officers are effectively elite policemen, and often perform personal protection duties for ministers, defence officials and even the President of the United States and his huge entourage. One trade secret that relates to this particular industry is highlighted in this feature - the wearing of a special insignia badge or crest. It is called a **HARD PIN.** During President Bush's state visit to the UK in 2003, US Secret Service agents and Scotland Yard officers wore a particular red badge. It was unique to this operation, and its bright colour, design, and reflective insignia was no coincidence. It is a signal to other security officers, watching British intelligence, and police officials that these men are there to help guard officials and dignitaries, such as the US Ambassador to Britain who also attended this London event. The crest will have been chosen at the last moment, and details of its design given to British security officers. This helps

prevent insurgency by an attacker, or a terrorist dressing and mimicking a Secret Service agent enabling him to get within striking distance of the VIP.

EXTRACT: The agent in the centre photograph (right), is also wearing another badge. This could mean he is a coordinator and is armed. It is also likely that the other agents would have been allowed to carry firearms because of the huge terrorist threat that exists against the UK and America. Also, the suits must not cloak or disguise the red badge, henceforth, note all the agents are wearing dark suits. The HARD PIN may be specially designed for key events...

TITLE: HOLDING YOUR NERVE

SUB TITLE: SPIES, AGENTS AND OPERATIVES IN THE FILED

ISSUE 21

INTRODUCTION:

"Whom did you work for... GRU, Spetsnaz or KGB?" asked the Canadian, in a light, but good natured tone. The Russian gentleman replied with a decisive, yet equally light tone: "No. I was a chess player." "Aren't those the most dangerous types?" asked another observer, with an English accent. The Russian gentleman smiled.

This might be a good time to start playing a piece of music by composer John Barry. Something intriguing! We are going to try and tackle that most difficult of questions: what makes the perfect spy. Alarm bells are already sounding... because, as the author to this thought provoking piece, I should point out that I possess no colourful espionage background. However, my chess game is improving and during the last ten years, with my exploration into self defence and related subjects, there have certainly been some interesting and sometimes spooky encounters. Some of my sources of information have also possessed very distinct backgrounds within that spider's web we call the security field. One of the fundamental difficulties of trying to determine what makes a good spy is the fact that there are so many different types of 'spy work' within the intelligence framework. So we need to recognise that the attributes most important to an accomplished spy within one field may be totally inappropriate in another.

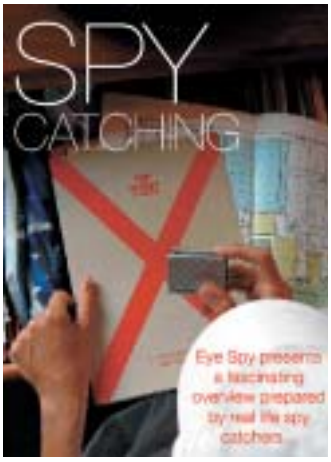
Even if we are to look at the most seemingly obvious requirements, there are contradictions. First, many government agencies stress integrity and loyalty as prerequisites for anyone wishing to serve their country within the intelligence setting. However, loyalty is a complex quality. *Does this mean loyalty to the state or loyalty to the organisation?* This is a question that might have challenged one former MI5 agent who sometimes enters the pages of Eye Spy.

Intelligence is something that would seem crucial if one wants to work within the various security services. Organisations such as the FBI and MI5 often recruit people with impressive academic backgrounds. In the past, Oxford and Cambridge have provided quite a few candidates for government recruiters. But today, an impressive academic background is not enough. Perhaps equally important is an individual's application of his or her intellectual capabilities....

TITLE: SPY CATCHING

SUB TITLE: HOW SPIES ARE CAUGHT

ISSUE 42



Espionage is said to be the second oldest profession. (For those who have to ask, the oldest is prostitution.) Like the oldest profession, the basics of espionage really haven't changed much over the past two thousand years. But there are a number of new developments in the kind of people involved, the information they seek and how they accomplish their shadowy task.

Experience is the best teacher, so some past cases have been selected and described to illustrate important points. Some timeless truths that need to be repeated may be best illustrated by older case files. Due to security, legal, privacy, and practical bureaucratic considerations, it usually

takes several years after an arrest and conviction before unclassified information on new cases becomes available for broad dissemination.

Espionage is a high-risk criminal offence. The traitor must fear arrest for the rest of his or her life. In the United States, for example, the statute of limitations does not apply to espionage, it's usually the same in most countries. Former National Security Agency employee Robert Lipka was arrested in 1996 - 30 years after he left NSA and 22 years after his last contact with Soviet intelligence.

There are four principal ways by which spies are detected: 1. Reporting by sources within a foreign intelligence service; 2. Routine counterintelligence monitoring; 3. Their own mistakes....

A fascinating insight into the world of real life spycatchers...

TITLE: SECRETS OF THE SPY TRADE 3

SUB TITLE: COUNTERMEASURES - THE SECRETS MOST SPIES DON'T WANT YOU TO KNOW

ISSUE 29

Kevin D. Murray presents a fascinating array of countermeasures used by the security services that will help thwart espionage, protect your company, household and yourself...

Who are the snoops?: Competitors, vendors, investigators, business intelligence consultants, colleagues vying for positions, overbearing bosses, suspicious partners, the press, labour negotiators, government agencies. The list is long.

Why would I be a target?: Money and power are the top two reasons behind illegal surveillance. If anything you say or write could increase someone else's wealth or influence, you are a target.

Is snooping common?: Yes. The news is full of stories about stolen information. In fact, many news stories themselves begin with leaks.

Can I protect myself?: Yes. Espionage is preventable. If you know the vulnerabilities, you can take the proper security precautions. Some spy tricks are obvious, if you stop to think about it. Some are clever abuses of the new technology we live with every day. All are devastating. Time has shown that many of the same tricks are used successfully over and over again. We present the top ten. Prepare to fight back.

Feature covers: Trash Trawling; Bugs and Wiretaps; Drop-by Spies; Hacking and Cracking; Cell Phone Leeches; Technology Traitors; Meeting Chameleons; The Silver Platter; Business Phone Attacks; Treason. And finally, what does a spy really look like?

How not to dress and drive. The operative is wearing a bright top, hat with distinct logo and not wearing a seat belt. The sunglasses are fine - as long as everyone else is wearing them

TITLE: DARK ARTS 4 - GHOST VEHICLES

SUB TITLE: TRADE SECRETS OF VEHICLE SURVEILLANCE

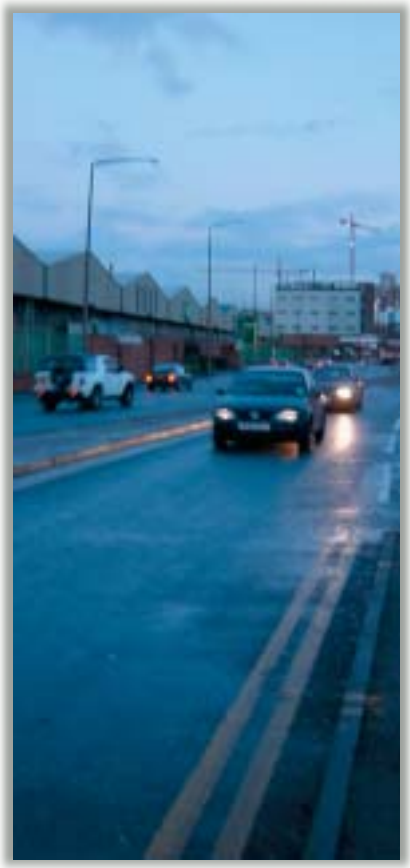
ISSUE 46

Despite what many people believe, following a vehicle is a precise art and one that cannot be learned overnight. If the driver of a target vehicle happens to be a criminal or worse - a terrorist, then the task is made even more dangerous, especially so if the surveillance is covert. There are numerous trade tips in this feature, including selection of vehicle, dress code, what to do in built-up areas, where to park, where not to park, communication skills, what to do if the target decides to journey on foot etc.


TRADECRAFT

GHOST VEHICLES

EXTRACT:



At some point in time in your driving career you will be asked by a friend, colleague or family member to "follow me." Depending on a variety of factors your journey will be easy, fairly easy, moderate, difficult... or impossible. Imagine therefore trying to follow a car without being seen for several hours. Add to that you must conduct a running commentary, and at some stage you might be asked to follow on foot. Ultimately, some government officers may also have to interact with the person under surveillance. For the security services, tracking a car covertly is at best complex. It's made particularly difficult if the driver or occupants in the target vehicle suspect they are under surveillance, or if the individual has colleagues performing anti-surveillance. The odds of an operation being compromised are lessened by correct vehicle selection, driving appropriately and communicating properly with colleagues.

Some analysts believe it's easier to track a car on an open road or motorway. Other surveillance officers think differently, and prefer to follow in built-up areas. The truth is, neither option is easy. Both scenarios can be affected by an array of situations. On a long motorway journey speed may be a factor; road traffic works can mean congestion and a slower pace. In an urban environment speeds are slower because of traffic lights, junctions, pedestrians, and increased traffic; the chance of losing sight of the vehicle increases dramatically if a surveillance driver loses concentration - even for a moment. This is one reason, but not the only one, why a professional surveillance operation will always involve several operatives and vehicles. At any point the suspect could stop and proceed on foot, thus vehicles will often carry more than one officer - just in case the surveillance has to be continued on foot. A second officer can provide commentary by radio, allowing the driver to focus on the road. He will deliver clear instructions calmly and without hesitation. Many surveillance vehicles now have the added bonus of satellite navigation systems, but professional operatives often avoid using these devices during an intense operation.

But the biggest threat to any surveillance is if the same vehicle is noticed on **multiple occasions.** Thankfully, by driving correctly and choosing the "right car", it's possible to avoid detection.

There are other lesser known factors which can ruin a vehicle surveillance. A chase car is equally as vulnerable when stationary or waiting for the target to depart. Not wearing a seat belt can attract attention. Parking on a yellow line (even briefly), may soon incur the wrath of a traffic warden. Sipping coffee or eating while at the wheel and in motion is distracting: in the UK, it's also illegal and if seen, the car will be stopped. Using a cell phone by hand or trying to find directions....

TITLE: TELEPHONE TAP COUNTER-MEASURES

SUB TITLE: WHAT CAN THE AVERAGE PERSON DO TO DISCOVER A TELEPHONE TAP

ISSUE 32

EXTRACT:

STOP! Don't buy that wiretap locator gadget from the mail-order catalogue. It's not effective. Don't call the experts to check your phone lines... well at least not yet. You are the average person. You're not involved in industrial espionage or government intrigue. You suspect an acquaintance, neighbour, or even a family member of being the culprit. You stand a good chance of discovering the eavesdropping device yourself. Basic wiretaps are just that - attachments to the telephone wires. Most amateur taps can be found just by looking at the wiring. There is no need to touch. In fact, you should never touch or tamper with unfamiliar wiring, or wiring which does not belong to you.

KNOW WHAT YOU ARE LOOKING AT

Household telephone wiring generally contains four pieces of wire in one cable. The cable is usually round. The inner pieces of wire are coloured: red, green, yellow and black. The red and green wires carry your calls. The yellow and black wires may be used for a second phone line, to carry power to...

TITLE: THE ART OF DISTRACTION

SUB TITLE:

ISSUE 48

Distraction - it's one of the most subtle, yet important weapons in the armoury of a spy, but increasingly some of this tradecraft used for hundreds of years is being adopted by terrorists, organised gangs and simple crooks. Eye Spy looks at the multifaceted tradecraft known as 'distraction'

The honest photo booth - a criminal's best friend. Once inside the user feels safe - but a bag placed on the floor is easy to remove.

EXTRACT ONE

One of the most common thefts - that at first seems to be the result of a local thug, occurs from public photo booths - usually located in busy shopping centres, train stations or large department stores. Adults use these outlets to acquire passports or driving licence photos. The booths themselves present a problem and many are quite simply "an accident waiting to happen" - for they are usually masked by only a three-quarter pull curtain, but they feel 'cosy' and once inside, the user feels safe from prying eyes. The booth in this case, is the actual distraction.

However, the trained criminal may wait for hours until he selects a target - usually a business person. Most people enter these booths and place their bag[s] on the floor. In a second it is easily pulled from under the curtain, and the thief disappears into the crowd... sometimes with enough information, and perhaps an old passport, credit cards, bill heads, address book, personal details etc. to create a new identity. **Never** place your bag on the floor; ask a friend to watch outside while the photos are being taken.

Major international crime gangs are often the most difficult to challenge. When drug cartels decide to move 200 million dollars of cocaine into Europe, for example, they will create a **parallel operation** that is described by Interpol as a distraction operation, albeit on a grandiose scale. If the ghost operation also works, then the outcome is a double success, if not, the loss is put down to 'collateral damage', and a few unimportant criminals will be caught. So how does it work?...

EXTRACT TWO

DISTRACTION IN AN OFFICE ENVIRONMENT

Acquiring intelligence from an office or secure complex is difficult enough, without the constant fear of being compromised. Those trained in tradecraft will use every known distraction technique to help secure intelligence. And there are many. A simple phone call to a desk official may cause him to leave his post, while a colleague slips by. The same trick can be used in an office environment, allowing access to a desk, computer or locker. If a longer period of time is necessary, a call may be made claiming his apartment has been broken into causing the person to head home quickly. If faced with this tactic, the subject should always remain calm, secure his desk or even call the police for confirmation. And don't take it as fact just because it is your superior who has told you - he may have received the bogus call himself. If it is essential a spy gains access to your home or office, he will research many aspects of your life - including your family, habits and travel arrangements. It might be easy to ignore criminal damage to your vehicle, but not so if 'auntie Edna' has just been rushed to a 'nearby hospital'....

Above: A typical purse snatch captured by Eye Spy. Subjects A stop a couple (Subjects B) and ask for directions or assistance. While engaged in the conversation, another member of the gang (Subject C) runs past and removes an item from the woman's bag - giving the impression she is hurrying to catch a bus

EXTRACT THREE

TERRORIST DISTRACTIONS

Today's terrorists are far more sophisticated than they ever were. This makes them unpredictable. Following the attacks on London in 2005 and New York in 2001, the streets of both these cities were flooded with heavily armed police and troops. Some members of the public called this an 'after-reaction', or 'too little too late'. It was neither. In both instances, the security services had no idea if further attacks were imminent. One incident in London may be the 'trigger' or call sign for another attack in New York. For example, within minutes of the 7 July 2005 bombings in London, security was tightened in New York, a move that saw hundreds of specialist officers deployed at specific sites across the city. Extra visible uniformed patrols were ordered and there was a general feeling that the 'ripples' from the London attacks may cross the Atlantic....

TITLE: BUGS - WHEN YOU NEED TO KNOW

SUB TITLE: NOTES ON COVERT RECORDING, BUGS AND COUNTERMEASURES

ISSUE 48

For those working in the intelligence or security business acquiring good quality audible data is an art: preparation is everything, though when the time comes to 'click' the record button, any one of a number of factors may conspire to dent your objective. Good fortune often plays a part, but an operative tasked with securing audio data will never rely totally on equipment. Machines are always liable to 'play up', but there are steps that can be taken to lessen the chance of failure. It's worth remembering also that in the intelligence game - there are occasions when an operation can be played out but once, and failure is not an option.

EXTRACT ONE

TAPPING AND TAPING

Successfully acquiring a warrant for a telephone intercept means that the security services can "listen and record" conversations on that line from a central station. In a growing investigation, it's likely that the authorities will need to monitor more lines. This is because other 'callers' or 'receivers' may become 'persons of interest'. All numbers are automatically identified and, if the data demands, a further electronic intercept warrant may be requested.

Faced with the task of tapping a telephone or intercepting an e-mail, the security services must endeavour to show good cause to apply for a warrant. And for those in America who believe its spy agencies are too active in this area look away now... the UK data may be simply too much to consume...

Nearly 440,000 official requests for communications' data were made by various UK agencies in a fifteen month period spanning 2005 - 2006. The requests' related to telephone calls, faxes, e-mails and ordinary letter post. The data, contained in the first report ever by the Interceptions of Communications Commissioner, also listed about 4,000 errors. The report's author - Sir Swinton Thomas, ended by saying the figure was "unacceptably high".

A bug - in this case a wall socket transmitter - can be fitted in minutes

EXTRACT TWO

In a lengthy surveillance (like the recent MI5 operation that led to the arrest of three 21/7 suspects), it's likely a variety of recorders and cameras were used. In this case, officers would have 'primed' locations frequented by the men, or at the very least, had them under observance. However, all transmitters are vulnerable once turned on. The signal can be detected and alert a target. Similarly, if an ordinary recorder (albeit security standard) is hidden in a location, it must be recovered, and this can often compromise an operation. Hidden transmitters are sometimes left in situ and no attempt is ever made to recover them. 'Super bugs' are the domain of the security services and huge corporations. These devices usually 'carry' their own countermeasures. If it senses a **'sweep'** is taking place, the device automatically shuts down and stops transmitting. They are rarely discovered....

EXTRACT THREE

If you suspect you are being bugged, and you can't find the device, then there are a few options available to you. **White Noise** will render most recordings useless. It's a type of noise that is produced by combining sounds of all different frequencies together. If you took all of the imaginable tones that a human can hear and combined them together, you would have white noise.

The adjective 'white' is used to describe this type of noise because of the way white light works. White light is light that is made up of all of the different colours (frequencies) of light combined together (a prism or a rainbow separates white light back into its component colours). In the same way, white noise is a combination of all of the different frequencies of sound. You can think of white noise as 20,000 tones all playing at the same time. Because white noise contains all frequencies, it is frequently used to mask other sounds. If you are in a hotel and voices from the room next-door are leaking into your room, you might turn on a fan to drown out the voices. The fan produces a good approximation of white noise.....

TITLE: TICKETS PLEASE

SUB TITLE: INTELLIGENCE GATHERING USING THE TICKET AND RECEIPT - WHAT SECRETS DO THEY HOLD?

ISSUE 41

If those intent on terrorism or criminal activity believe their only 'enemies' are the police, CCTV cameras, security services or law abiding members of the public, think again. The intelligence world has a plethora of people, tools and 'tricks of the trade' to gather vital information on subjects under surveillance - it also has two unlikely friends - the ticket and receipt...

EXTRACT:

It comes in all shapes and sizes; some are about two inches square, while others, such as airline booking forms printed from the internet, are as large as the paper you are reading. Its material value is worthless, but a ticket, and more importantly, the data contained within, is priceless to the intelligence world. For investigators searching train wreckage after the 7 July London atrocities, finding such items proved spectacular. Tickets purchased at various stations (and recovered from the bodies of the bombers) led the police all the way to Luton, and the recovery of even more explosives. Ticket analysis on a vehicle recovered at the car park in Luton station provided more data. Soon the trail led back to Leeds and quite quickly all four terrorists were identified. Within hours the 'bomb factory' had been found and further investigations ensued. But what are the authorities looking for?

Each train and tube ticket contains priceless data. Officers can determine when and where a purchase was made. They immediately examine what type of journey can be made with each ticket. A 'return ticket', for example, could provide clues to the subject's ambitions; others may help identify what stations the train stopped at. It's valuable, if not laborious data to explore.

PLUS: GOVERNMENT RULES AND REGULATIONS ON SURVEILLANCE - Everything you need to know on what's legal and what's not relating to surveillance

TITLE: ACOUSTICAL ESPIONAGE

SUB TITLE:

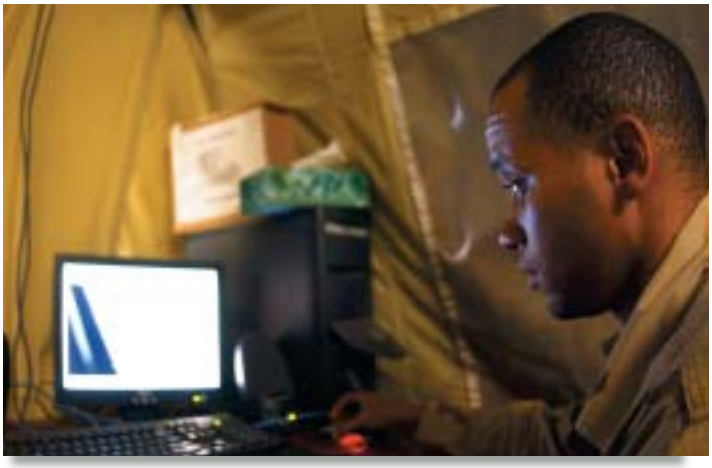
ISSUE 36

It's a fascinating form of tradecraft and essential for those who work in the intelligence business to understand...

EXTRACT:

Already dubbed "acoustical spying", researchers took several 10-minute sound recordings of users typing at a keyboard. The audio tapes were then fed into a computer and astonishingly the programme recovered 96 per cent of the characters entered.

"It's a form of acoustical spying that should raise red flags among computer security and privacy experts," said Doug Tygar, UC Berkeley professor of computer science and information management and principal investigator of the study. "If we were able to figure this out, it's likely that



Passwords and the forwarding of secret - typed information is vulnerable if the system can audibly record the key strokes. Tape recorders do not necessarily have to be in the immediate area - a parabolic mic recording is just as effective

people with less honourable intentions can - or have - as well."

Each keystroke makes a relatively distinct sound. The sound signature remains the same regardless of how hard a key is struck or the speed in which it is entered.

"Typical users type about 300 characters per minute, leaving enough time for a computer to isolate the sounds of individual key-strokes and categorise the letters based upon the statistical characteristics of English text. For example, the letters 'th' will occur together more frequently than 'tj,' and the word 'yet' is far more common than 'yrg'.

"Using statistical learning theory, the computer can categorise the sounds of each key as it's struck and develop a good first guess with an accuracy of 60 percent for characters, and 20 percent for words," said Li Zhuang, a UC Berkeley Ph.D. student in computer science and lead author of the study. "We then use spelling and grammar checks to refine the results, which increased the character accuracy to 70 percent and the word accuracy to 50 percent. The text is somewhat readable at this point."

The recording is then played back repeatedly in a feedback loop to 'train' the computer to increase its accuracy until no significant improvement is seen....